The background of the slide is a screenshot of the Wireshark network protocol analyzer. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, search, and analysis. A filter bar at the top right shows 'Apply a display filter ... <Ctrl-/>' and 'Expression...'. The main display area is a large yellow rectangle containing the event information. At the bottom, a status bar shows 'algar' on the left and 'Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 | Profile: Default' on the right.

IX (PTT) Fórum 11

04 e 05 de Dezembro de 2017

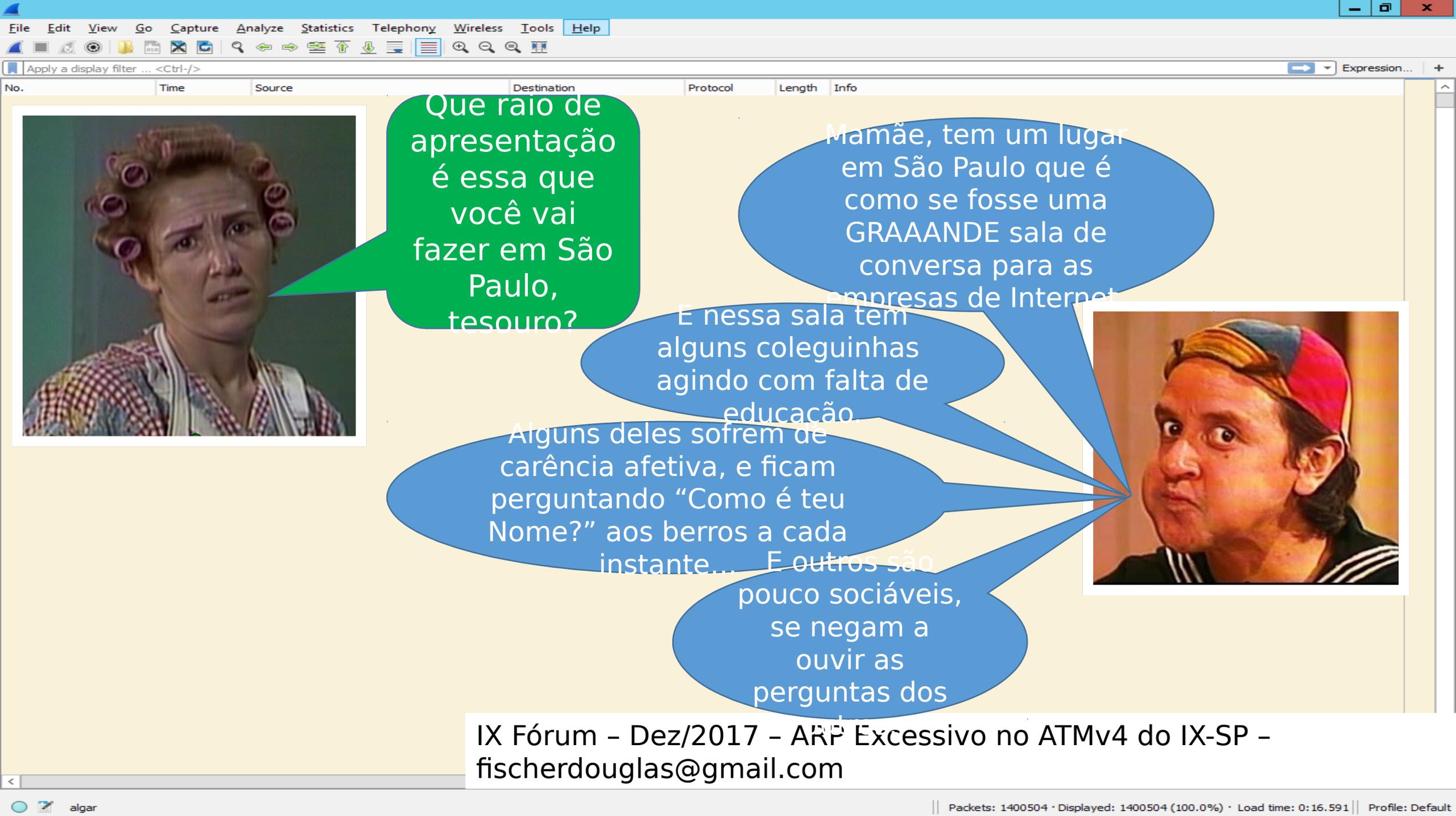
ARP excessivo no barramento do ATMv4 do IX-SP
Análise de causas, problemas e possíveis soluções

Autor: Douglas Fernando Fischer -
fischerdouglas@gmail.com

Douglas Fernando Fischer

- Engenheiro de Controle e Automação
- Atua na área de redes de telecomunicações desde 1999
- Trabalhou como engenheiro de pré-vendas e implantação em integradores de tecnologia
- Consultor na área de redes e servidores no segmento corporativo e provedores de Internet
- Unioeste - Responsável pela área de Routing e Switching
- Tretísta com fins produtivos nas horas vagas

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com



Que raio de apresentação é essa que você vai fazer em São Paulo, tesouro?

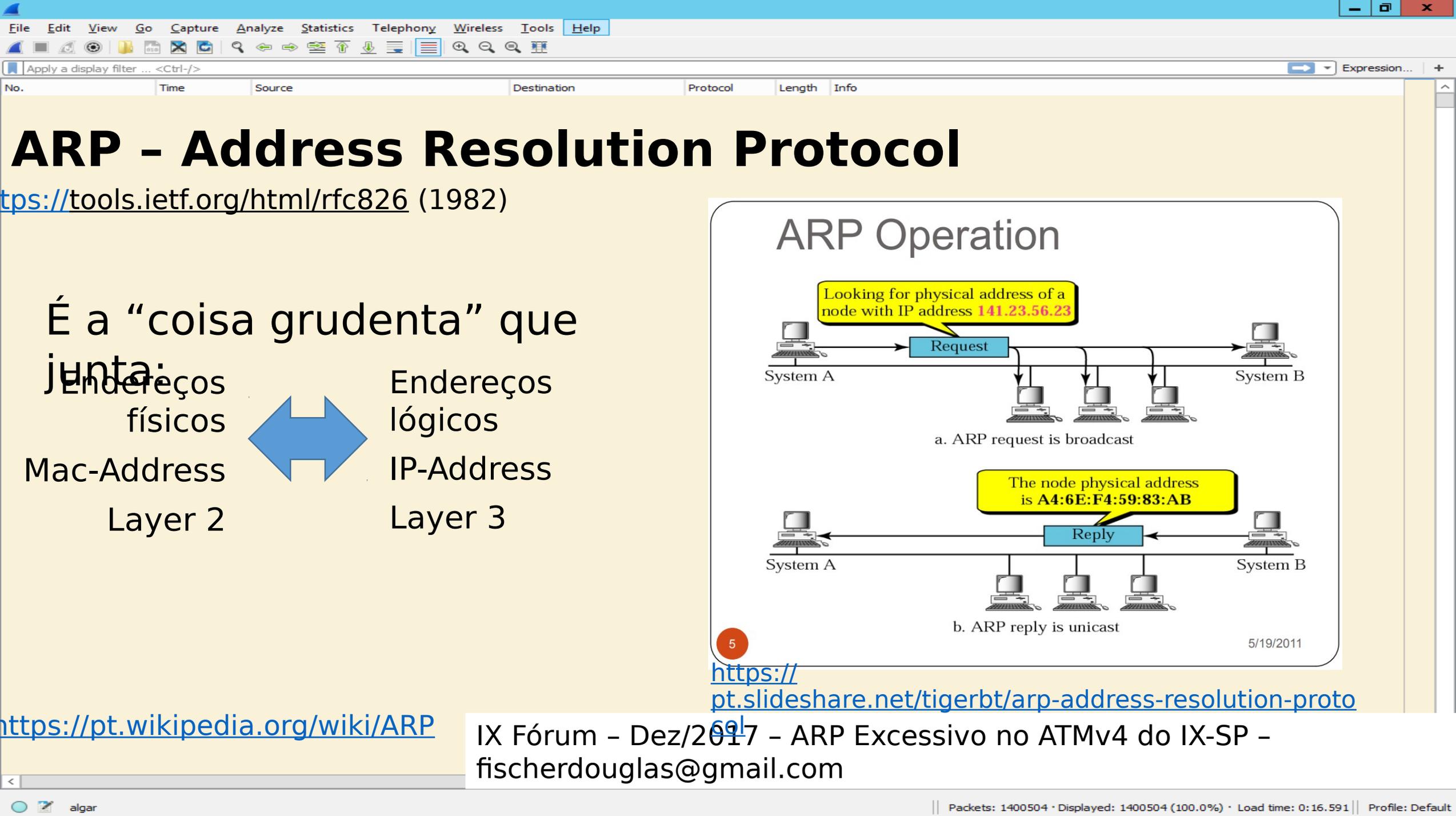
Mamãe, tem um lugar em São Paulo que é como se fosse uma GAAANDE sala de conversa para as empresas de Internet

E nessa sala tem alguns coleguinhas agindo com falta de educação.

Alguns deles sofrem de carência afetiva, e ficam perguntando "Como é teu Nome?" aos berros a cada instante...

E outros são pouco sociáveis, se negam a ouvir as perguntas dos

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com



ARP - Address Resolution Protocol

<https://tools.ietf.org/html/rfc826> (1982)

É a “coisa grudenta” que

junta:

Endereços físicos

Mac-Address

Layer 2

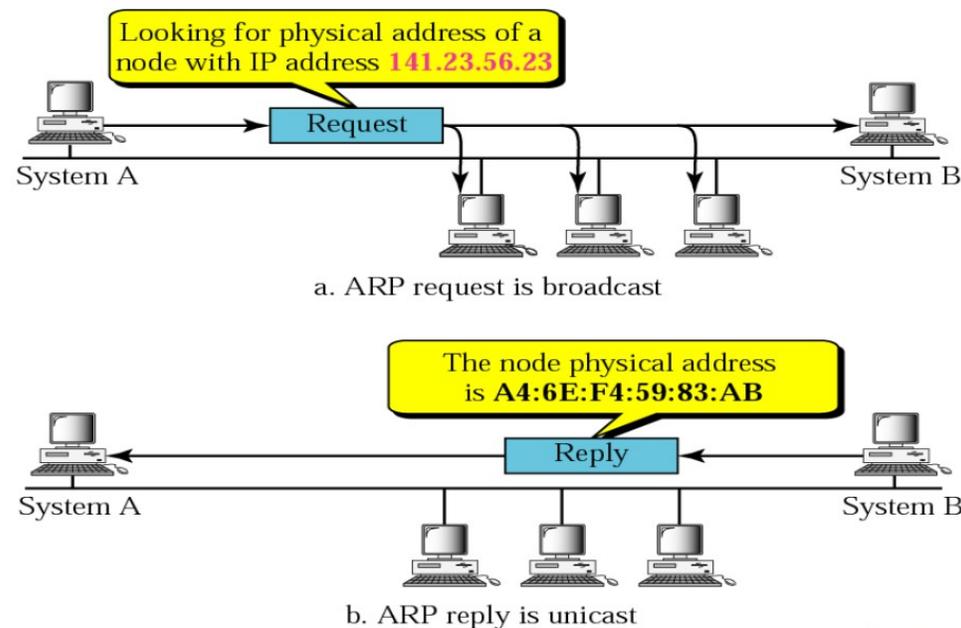


Endereços lógicos

IP-Address

Layer 3

ARP Operation



5

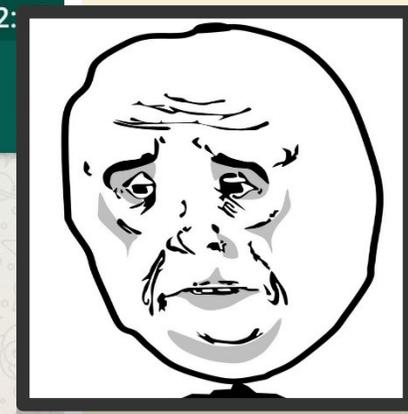
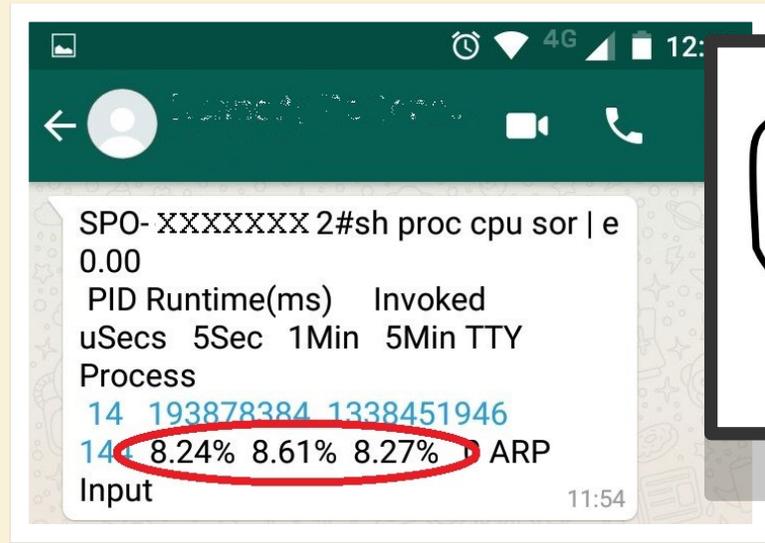
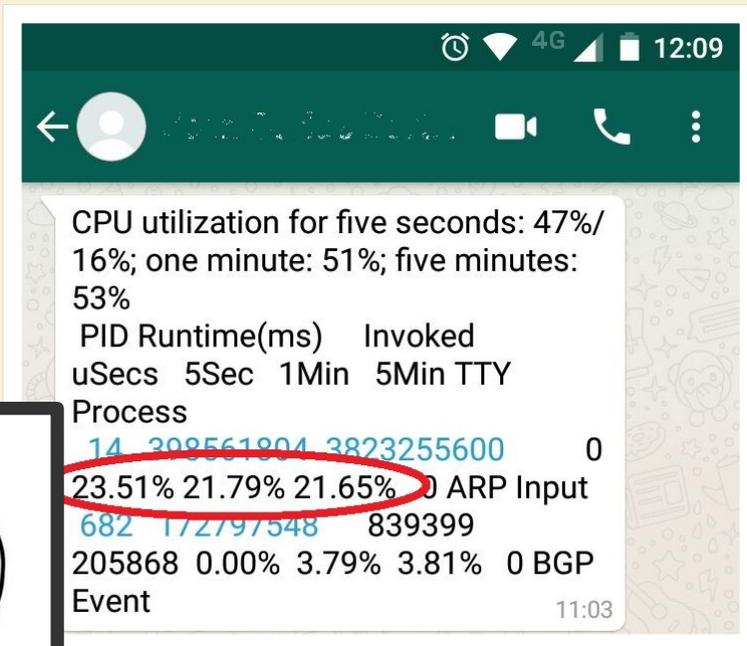
<https://pt.slideshare.net/tigerbt/arp-address-resolution-protocol>

<https://pt.wikipedia.org/wiki/ARP>

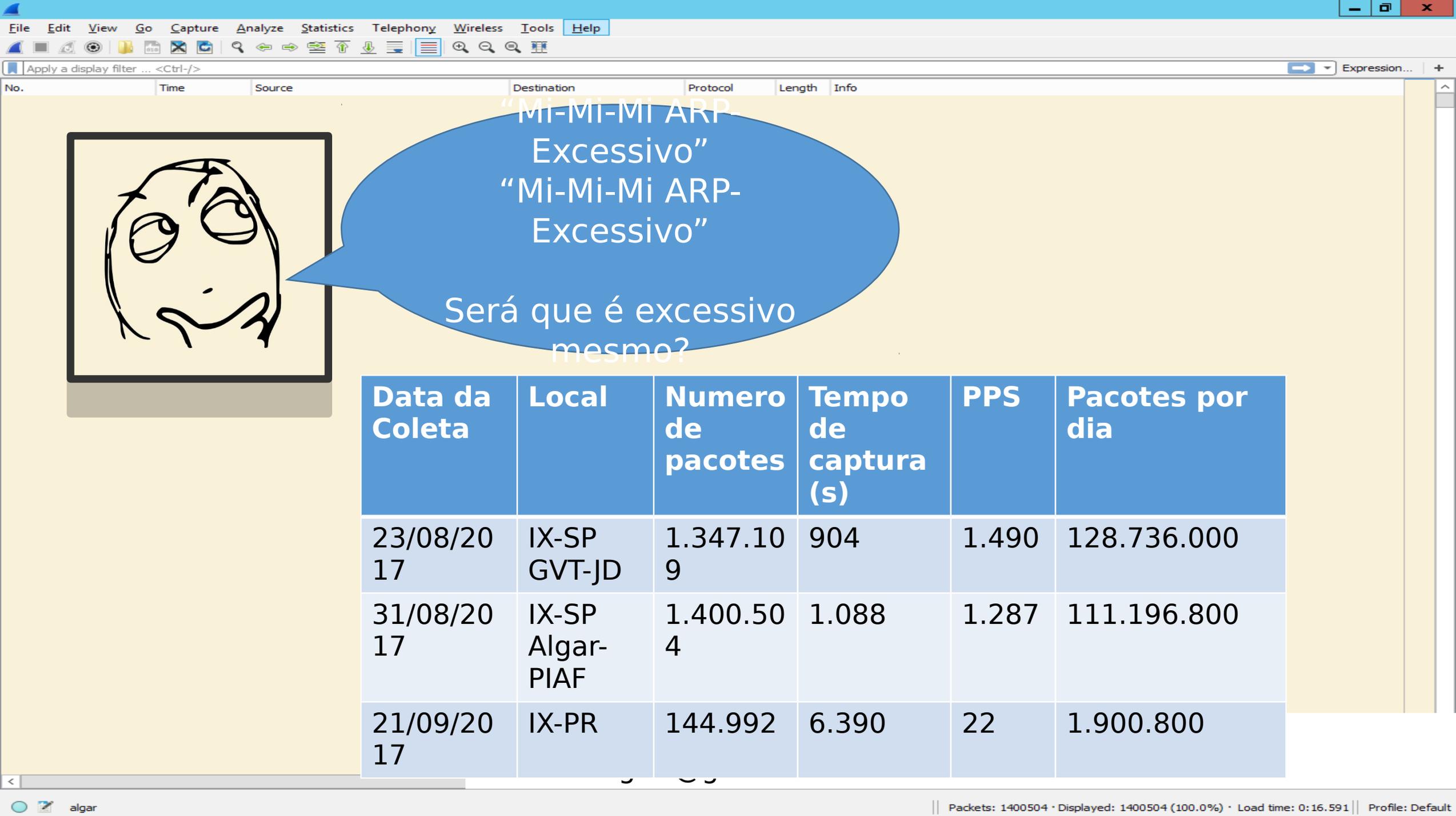
IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com

Como essa encrenca caiu no meu colo?

Software-based vs Hardware-based Routers



IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com



"MI-MI-MI ARP Excessivo"
"MI-MI-MI ARP-Excessivo"

Será que é excessivo mesmo?

Data da Coleta	Local	Numero de pacotes	Tempo de captura (s)	PPS	Pacotes por dia
23/08/2017	IX-SP GVT-JD	1.347.109	904	1.490	128.736.000
31/08/2017	IX-SP Algar-PIAF	1.400.504	1.088	1.287	111.196.800
21/09/2017	IX-PR	144.992	6.390	22	1.900.800

Não é a primeira vez que escutam os falar sobre problemas com ARP no PTT-SPO.

[GTER] PTT-SP, arp-request sem arp-reply

- | Nome | Tempo | Destino | Protocolo | Comprimento | Info |
|--------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------|------|
| Paulo Henrique | 23/02 | Bom dia pessoal, a cerca de dois dias identificamos em nossa estrutura uma si... | | | |
| Rubens Kuhl | 23/02 | Sem nenhum de tipo de redundância como CARP, VRRP etc. ? Eles utilizam CARP, ... | | | |
| Idd@starweb.com.br | 24/02 | Olá, Ja tive este problema 3 vezes no PTT, foi resolvido dando um shutdown e ... | | | |
| Danton Nunes | 24/02 | veja este artiguinho: http://www.royong.com/showthread.php?t=5134 talvez seja... | | | |
| Douglas Fischer | 25/02 | O primeiro problema que me veio a cabeça foi justamente o uso de algum FHRP, ... | | | |
| MrGuga | 25/02 | Tivemos problema semelhante no PTT-RS e era um filtro mal-feito do nosso lado... | | | |
| Paulo Henrique | 26/02 | Bom dia pessoal, vamos lá. Sim, nenhum tipo de redundância - pelo menos do no... | | | |
| Paulo Henrique | 26/02 | Hum, interessante, vou considerar isso. Obrigado. >> gter list https://eng.re... | | | |
| Paulo Henrique | 26/02 | Obrigado Danton, mas tudo leva a crer que não é este o problema. Os logs não ... | | | |
| Paulo Henrique | 26/02 | Realmente, este não parece ser o nosso caso. | | | |
| Paulo Henrique | 26/02/2013 | Fiz um levantamento e procurei encontrar algum mac como você disse mas não en... | | | |

Paulo Henrique paulohenriquef@gmail.com por_eng.registro.t 20/03/2013 ★
para Grupo

Pessoal, como o assunto acabou voltando a ser levantado na lista e eu ainda não havia postado nada até hoje, resolvi então escrever para relatar nossa situação atual.
Depois de muitas buscas acabei me deparando com este material do Amsterdam Internet Exchange:

<https://www.ams-ix.net/technical-specifications-descriptions/config-guide#11>

Como eu havia dito, utilizamos linux como roteador, então, fiz as seguintes configurações:

```
net.ipv4.neigh.IF_XXX.base_reachable_time = 14400  
net.ipv4.neigh.IF_XXX.gc_stale_time = 1200
```

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com

Também não
somos os
primeiros do
mundo a sofrer
com isso.

Amsterdam Internet Exchange

Seguro | https://ams-ix.net/technical/specifications-descriptions/controlling-arp-traffic-on-ams-ix-platform

Other AMS-IX Exchanges My AMS-IX

amsix

Connect to AMS-IX Services & Pricing Technical Connected networks About

Contact FAQ

Technical

- AMS-IX Infrastructure
The AMS-IX MPLS/VPNS infrastructure
- Specifications & Descriptions
 - Allowed traffic
 - Config guide
 - IPv6 Numbering Scheme
 - Port security at AMS-IX
 - Quarantine VLAN
 - Interface & cabling specifications
 - Link aggregation
 - Quality Statement
 - AS1200 peering
 - sFlow at AMS-IX
 - AMS-IX Route Servers
 - Dynamic per-AS
 - Prefix Limits
 - Falcon class Route Servers
 - Controlling ARP Traffic on AMS-IX platform
- Statistics
 - Colocation traffic
 - Real Time Stats
 - sFlow Stats
 - Frame size

Controlling ARP Traffic on AMS-IX platform

1. ARP (Address Resolution Protocol)

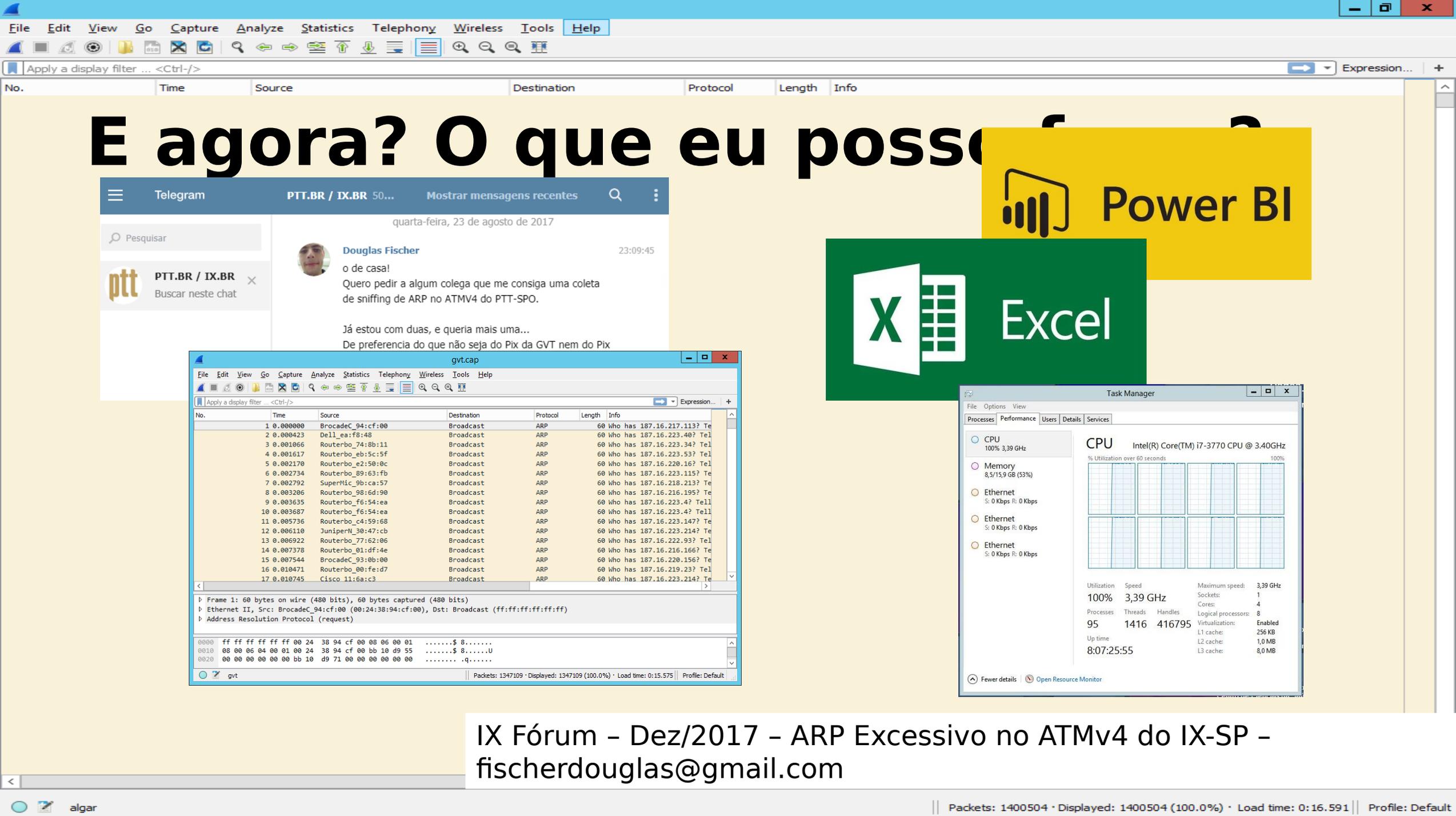
ARP (Address Resolution Protocol) is the Layer-2 protocol used by AMS-IX member's router to associate IPv4 address with the MAC address of peers interfaces.

[More about ARP](#)
2. Problems caused by too much ARP traffic

On Ethernet networks, the Address Resolution Protocol (ARP) is used to find the MAC-address for a given IPv4 address. ARP uses Ethertype 0x0806 together with Ethernet broadcasting. A node will broadcast an ARP Request packet to ask for the MAC address of an unknown IPv4address. The node using the requested IP address replies (using regular unicast) with an ARP Reply packet, which includes its MAC address. In order to work, it is important that all nodes using IPv4 listen for ARP packets and reply to them if necessary. The nodes therefore need to process all Ethernet broadcast messages with Ethertype 0x0806. For each ARP packet, they must decide whether or not to reply. Processing ARP packets can take a lot of processing power. Because all ARP packets need to be examined in order for ARP to work, processing ARP packets may take precedence over other activities, depending on the Operating System. As such, when there is a lot of ARP traffic, routers may be unable to do other processing tasks like maintaining BGP sessions. This problem was noticed on AMS-IX when the ISP peering LAN was renumbered to new IPv4 addresses. Members in the new IPv4 range were trying to reach members in the old IPv4range and vice versa. Larger amounts of ARP packets than usual crossed the network, consuming all available processing power on some customer routers, not leaving enough to process BGP in a timely manner, resulting in lost BGP sessions. Other routers started sending ARP packets to re-establish these BGP sessions, resulting in an ARP storm that brought even more routers down.
3. ARP Sponge – the AMS-IX solution

To help routers survive heavy ARP traffic, AMS-IX decided to try keeping the amount of ARP traffic down. For this purpose, AMS-IX developed a daemon, written in Perl, called ARP Sponge. The ARP Sponge listens on the ISP

IX Fórum – Dez/2017 – ARP Excessivo no ATMv4 do IX-SP –
fischerdouglas@gmail.com



E agora? O que eu posso fazer?

Telegram PTT.BR / IX.BR 50... Mostrar mensagens recentes

quarta-feira, 23 de agosto de 2017

Douglas Fischer 23:09:45

o de casa!
Quero pedir a algum colega que me consiga uma coleta de sniffing de ARP no ATMv4 do PTT-SPO.

Já estou com duas, e queria mais uma...
De preferencia do que não seja do Pix da GVT nem do Pix



gvt.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	BrocadeC_94:cf:00	Broadcast	ARP	60	who has 187.16.217.113? Te
2	0.000423	Dell_ea:f8:48	Broadcast	ARP	60	who has 187.16.223.40? Tel
3	0.001066	Routerbo_74:8b:11	Broadcast	ARP	60	who has 187.16.223.34? Tel
4	0.001617	Routerbo_eb:5c:5f	Broadcast	ARP	60	who has 187.16.223.53? Tel
5	0.002170	Routerbo_e2:50:0c	Broadcast	ARP	60	who has 187.16.220.16? Tel
6	0.002734	Routerbo_89:63:fb	Broadcast	ARP	60	who has 187.16.223.115? Te
7	0.002792	SuperMic_9b:ca:57	Broadcast	ARP	60	who has 187.16.218.213? Te
8	0.003206	Routerbo_98:6d:90	Broadcast	ARP	60	who has 187.16.216.195? Te
9	0.003635	Routerbo_f6:54:ea	Broadcast	ARP	60	who has 187.16.223.4? Tel1
10	0.003687	Routerbo_f6:54:ea	Broadcast	ARP	60	who has 187.16.223.4? Tel1
11	0.005736	Routerbo_c4:59:68	Broadcast	ARP	60	who has 187.16.223.147? Te
12	0.006110	JuniperN_30:47:cb	Broadcast	ARP	60	who has 187.16.223.214? Te
13	0.006922	Routerbo_77:62:06	Broadcast	ARP	60	who has 187.16.222.93? Tel
14	0.007378	Routerbo_01:df:4e	Broadcast	ARP	60	who has 187.16.216.166? Te
15	0.007544	BrocadeC_93:0b:00	Broadcast	ARP	60	who has 187.16.220.156? Te
16	0.010471	Routerbo_00:fe:d7	Broadcast	ARP	60	who has 187.16.219.23? Tel
17	0.010745	Cisco_11:6a:c3	Broadcast	ARP	60	who has 187.16.223.214? Te

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: BrocadeC_94:cf:00 (00:24:38:94:cf:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

```

0000  ff ff ff ff ff ff 00 24 38 94 cf 00 08 06 00 01  .....$ 8.....
0010  08 00 06 04 00 01 00 24 38 94 cf 00 bb 10 d9 55  .....$ 8.....U
0020  00 00 00 00 00 00 bb 10 d9 71 00 00 00 00 00 00  ..... .q.....

```

Task Manager

CPU 100% 3,39 GHz

Memory 8,5/15,9 GB (53%)

Ethernet S: 0 Kbps R: 0 Kbps

Ethernet S: 0 Kbps R: 0 Kbps

Ethernet S: 0 Kbps R: 0 Kbps

Utilization: 100% Speed: 3,39 GHz Maximum speed: 3,39 GHz

Processes: 95 Threads: 1416 Handles: 416795

Up time: 8:07:25:55

Sockets: 1
Cores: 4
Logical processors: 8
Virtualization: Enabled
L1 cache: 256 KB
L2 cache: 1,0 MB
L3 cache: 8,0 MB

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglas@gmail.com

Primeiras Análises (23/08/2017)

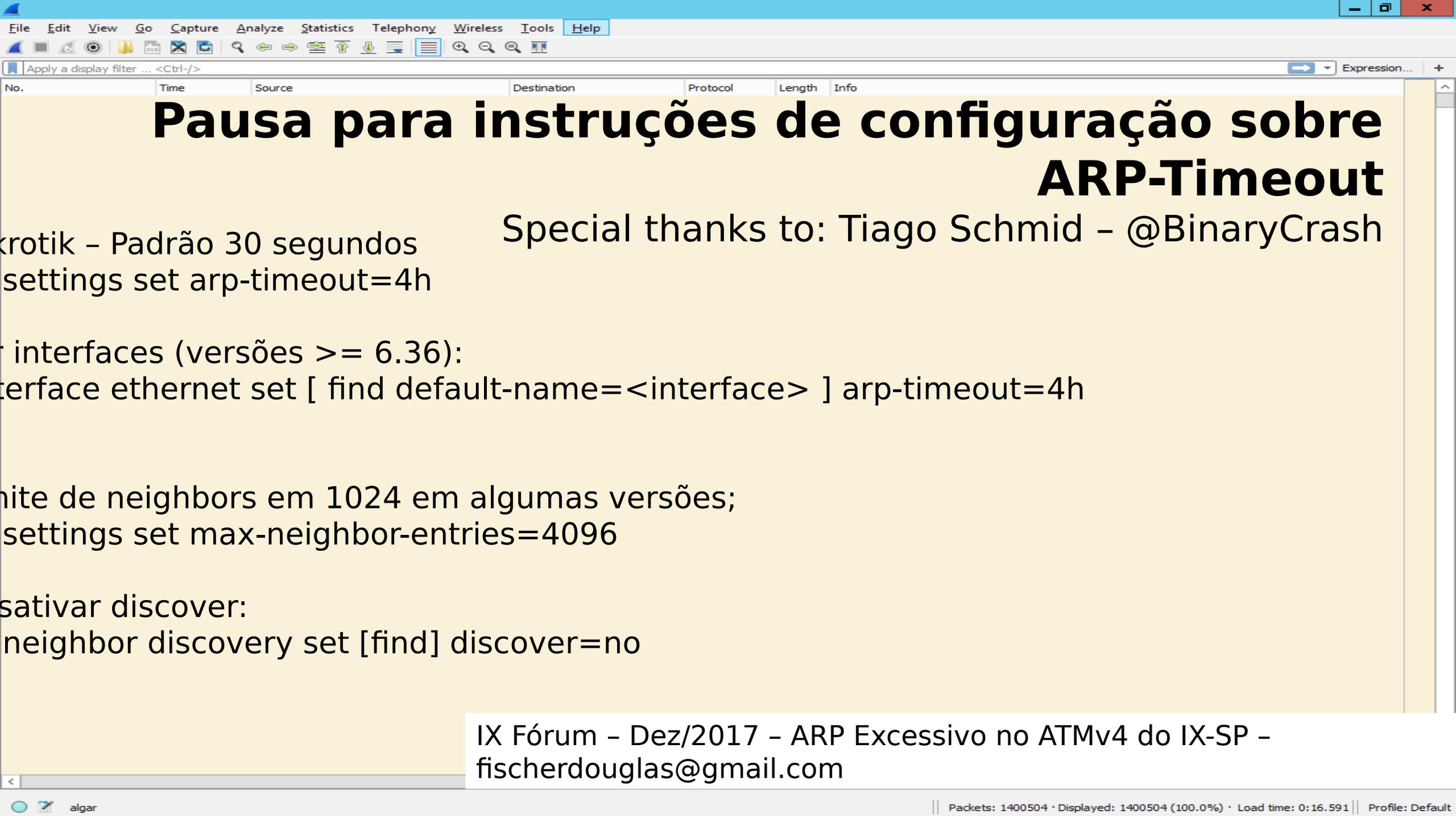


Análise dos pacotes de Brodcasts transmitidos no IX-SP
Capturas realizadas em multiplos PIX em 23/08/2017

Fabricante	% requests Emitidos	Fabricante	% requests procurados	Fabricante	Qtde. part. por EUI	% Relativo
Routerbo	56,25%	Routerbo	30,15%	Routerbo	624	44,86%
JuniperN	12,70%	(vazio)	21,00%	JuniperN	267	19,19%
Dell	5,99%	JuniperN	16,76%	Cisco	92	6,61%
IntelCor	5,87%	HuaweiTe	10,14%	IntelCor	81	5,82%
Cisco	5,54%	Cisco	8,64%	Ubiquiti	50	3,59%
Ubiquiti	3,15%	IntelCor	3,39%	Dell	44	3,16%
BrocadeC	2,01%	Serveru	1,93%	HuaweiTe	39	2,80%
Broadcom	1,75%	Ubiquiti	1,87%	Serveru	29	2,08%
Serveru	1,29%	Dell	1,30%	Broadcom	23	1,65%
Vmware	0,81%	HewlettP	0,57%	Trendnet	22	1,58%
Ibm	0,62%	SuperMic	0,55%	Ibm	16	1,15%
AristaNe	0,55%	ChelsioC	0,41%	HewlettP	12	0,86%
SuperMic	0,49%	LannerEl	0,40%	BrocadeC	12	0,86%
HuaweiTe	0,45%	Vmware	0,39%	LannerEl	11	0,79%
AxiomTec	0,44%	BrocadeC	0,35%	SuperMic	9	0,65%

<https://drive.google.com/file/d/0B2ezIM5Mir8PbE9LbE1TRmRuaUU/view>

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com



Pausa para instruções de configuração sobre ARP-Timeout

Special thanks to: Tiago Schmid - @BinaryCrash

```
 Mikrotik - Padrão 30 segundos  
 settings set arp-timeout=4h
```

```
 r interfaces (versões >= 6.36):
```

```
 r interface ethernet set [ find default-name=<interface> ] arp-timeout=4h
```

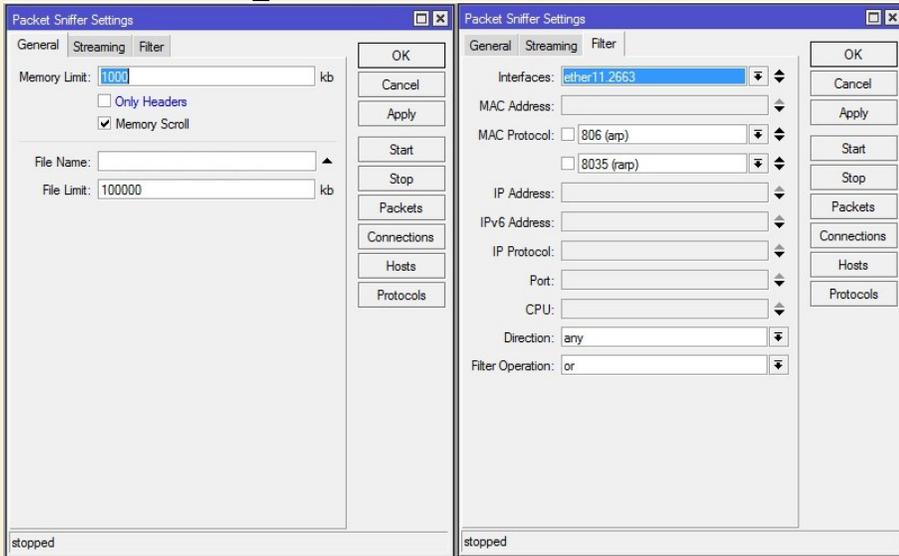
```
 nte de neighbors em 1024 em algumas versões;  
 settings set max-neighbor-entries=4096
```

```
 sativar discover:
```

```
 neighbor discovery set [find] discover=no
```

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

OK, mas isso não define completamente as causas...



Mais coletas, mais Wireshark, mais Excel, mais tabela dinâmica...

Vários agradecimentos são necessários!
Especial ao Cristofer Velloso

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

Então pude fazer algumas análises (31/08/2017)

[GTER] IX Broadcast - Sugestão - Broadcast Clearing vs ARP Sponge

Douglas Fischer [fischerdouglas at gmail.com](mailto:fischerdouglas@gmail.com)
Fri Sep 1 01:39:38 BRT 2017

- Next message (by thread): [\[GTER\] IX Broadcast - Sugestão - Broadcast Clearing vs ARP Sponge](#)
- Messages sorted by: [\[date\]](#) [\[thread\]](#) [\[subject\]](#) [\[author\]](#)

Acabo de concluir mais uma análise de Sniffing de ARP na Vlan do ATM do IX-SP.

<https://eng.registro.br/pipermail/gter/2017-September/071371.html>

Estendi mais a análise, com maior foco no destino, e acredito que consegui matar uma das charadas do problema!

<https://eng.registro.br/pipermail/gter/2017-September/071380.html>

IX Fórum - De
fischerdouglas

Seguem os links para os arquivos:

SniffingARP-IX-SP_2017-08-31_ConfiguraçõesIncoerentes.pdf

<https://drive.google.com/open?id=0B2ezIM5Mir8PVGViY3JSc0xMX1E>

SniffingARP-IX-SP_2017-08-31_ResumoPorFabricante.pdf

<https://drive.google.com/open?id=0B2ezIM5Mir8PenBHN18yWDNtdnc>

SniffingARP-IX-SP_2017-08-31_ResumoPorIPProcurado.pdf

<https://drive.google.com/open?id=0B2ezIM5Mir8PUjZPOEjzM3NGMEE>

SniffingARP-IX-SP_2017-08-31_ResumoPorIPProcurador.pdf

<https://drive.google.com/open?id=0B2ezIM5Mir8PNjjPTXNfUmlxLTg>

SniffingARP-IX-SP_2017-08-31_SemDadosDaColeta.xlsx (631KB)

<https://drive.google.com/open?id=0B2ezIM5Mir8PT01nUDRzVTBmWDA>

SniffingARP-IX-SP_2017-08-31.xlsx (49,9MB)

<https://>

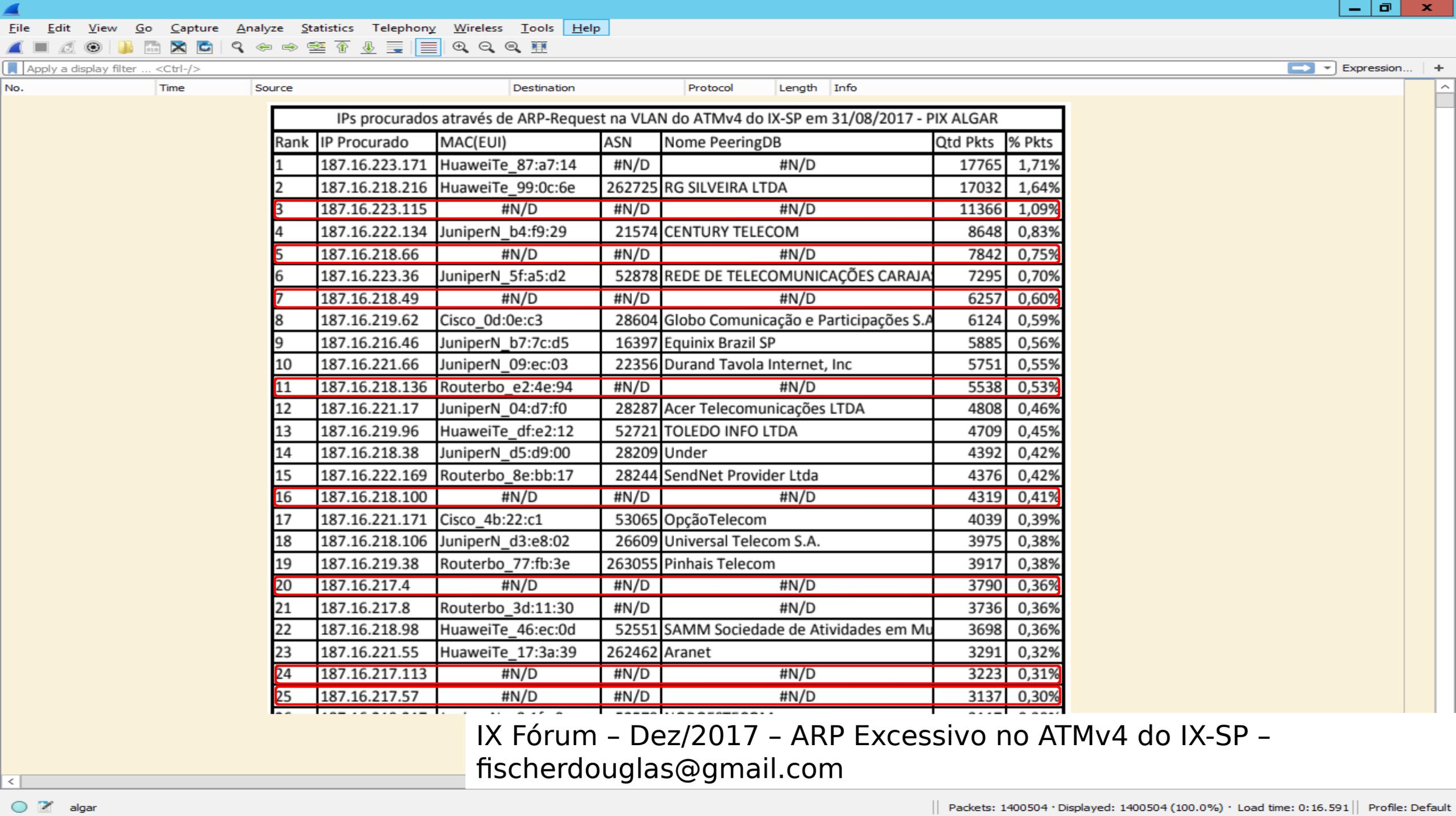
Dados obtidos através de Sniffing de Pacotes ARP Na Vlan do IX-SP em 31/08/2017 em porta conectada ao PIX da Algar

ARP- Procuradores			
	MAC(EUI)	Qtd Pkts	% Pkts
1	Routerbo	592794	56,91%
2	JuniperN	130553	12,53%
3	Cisco	74231	7,13%
4	IntelCor	55977	5,37%
5	Dell	33693	3,23%
6	Serveru	26666	2,56%
7	BrocadeC	24225	2,33%
8	Ubiquiti	24141	2,32%
9	Broadcom	16819	1,61%
10	SuperMic	7819	0,75%

ARP - Procurados			
	MAC(EUI)	Qtd Pkts	% Pkts
1	Routerbo	303878	29,17%
2	#N/D	302170	29,01%
3	JuniperN	179692	17,25%
4	HuaweiTe	72951	7,00%
5	Cisco	47541	4,56%
6	IntelCor	38788	3,72%
7	Serveru	20092	1,93%
8	Ubiquiti	20009	1,92%
9	Dell	11607	1,11%
10	HewlettP	4743	0,46%

Proporção Vendors			
	MAC(EUI)	Qtd Partic.	% Partic.
1	Routerbo	616	48,50%
2	JuniperN	245	19,29%
3	IntelCor	76	5,98%
4	Cisco	71	5,59%
5	Ubiquiti	44	3,46%
6	HuaweiTe	31	2,76%
7	Dell	32	2,52%
8	Serveru	28	2,20%
9	Broadcom	15	1,18%
10	BrocadeC	12	0,94%

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com



IPs procurados através de ARP-Request na VLAN do ATMv4 do IX-SP em 31/08/2017 - PIX ALGAR

Rank	IP Procurado	MAC(EUI)	ASN	Nome PeeringDB	Qtd Pkts	% Pkts
1	187.16.223.171	HuaweiTe_87:a7:14	#N/D	#N/D	17765	1,71%
2	187.16.218.216	HuaweiTe_99:0c:6e	262725	RG SILVEIRA LTDA	17032	1,64%
3	187.16.223.115	#N/D	#N/D	#N/D	11366	1,09%
4	187.16.222.134	JuniperN_b4:f9:29	21574	CENTURY TELECOM	8648	0,83%
5	187.16.218.66	#N/D	#N/D	#N/D	7842	0,75%
6	187.16.223.36	JuniperN_5f:a5:d2	52878	REDE DE TELECOMUNICAÇÕES CARAJA	7295	0,70%
7	187.16.218.49	#N/D	#N/D	#N/D	6257	0,60%
8	187.16.219.62	Cisco_0d:0e:c3	28604	Globo Comunicação e Participações S.A	6124	0,59%
9	187.16.216.46	JuniperN_b7:7c:d5	16397	Equinix Brazil SP	5885	0,56%
10	187.16.221.66	JuniperN_09:ec:03	22356	Durand Tavola Internet, Inc	5751	0,55%
11	187.16.218.136	Routerbo_e2:4e:94	#N/D	#N/D	5538	0,53%
12	187.16.221.17	JuniperN_04:d7:f0	28287	Acer Telecomunicações LTDA	4808	0,46%
13	187.16.219.96	HuaweiTe_df:e2:12	52721	TOLEDO INFO LTDA	4709	0,45%
14	187.16.218.38	JuniperN_d5:d9:00	28209	Under	4392	0,42%
15	187.16.222.169	Routerbo_8e:bb:17	28244	SendNet Provider Ltda	4376	0,42%
16	187.16.218.100	#N/D	#N/D	#N/D	4319	0,41%
17	187.16.221.171	Cisco_4b:22:c1	53065	OpçãoTelecom	4039	0,39%
18	187.16.218.106	JuniperN_d3:e8:02	26609	Universal Telecom S.A.	3975	0,38%
19	187.16.219.38	Routerbo_77:fb:3e	263055	Pinhais Telecom	3917	0,38%
20	187.16.217.4	#N/D	#N/D	#N/D	3790	0,36%
21	187.16.217.8	Routerbo_3d:11:30	#N/D	#N/D	3736	0,36%
22	187.16.218.98	HuaweiTe_46:ec:0d	52551	SAMM Sociedade de Atividades em Mu	3698	0,36%
23	187.16.221.55	HuaweiTe_17:3a:39	262462	Aranet	3291	0,32%
24	187.16.217.113	#N/D	#N/D	#N/D	3223	0,31%
25	187.16.217.57	#N/D	#N/D	#N/D	3137	0,30%

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com

IPs procurados através de ARP-Request na VLAN do ATMv4 do IX-SP em 31/08/2017 - PIX ALGAR						
Rank	IP Procurado	MAC(EUI)	ASN	Nome PeeringDB	Qtd Pkts	% Pkts
1	187.16.223.171	HuaweiTe_87:a7:14	#N/D	#N/D	17765	1,71%
2	187.16.218.216	HuaweiTe_99:0c:6e	262725	RG SILVEIRA LTDA	17032	1,64%
4	187.16.222.134	JuniperN_b4:f9:29	21574	CENTURY TELECOM	8648	0,83%
6	187.16.223.36	JuniperN_5f:a5:d2	52878	REDE DE TELECOMUNICAÇÕES CARAJA	7295	0,70%
8	187.16.219.62	Cisco_0d:0e:c3	28604	Globo Comunicação e Participações S.A	6124	0,59%
9	187.16.216.46	JuniperN_b7:7c:d5	16397	Equinix Brazil SP	5885	0,56%
10	187.16.221.66	JuniperN_09:ec:03	22356	Durand Tavola Internet, Inc	5751	0,55%
11	187.16.218.136	Routerbo_e2:4e:94	#N/D	#N/D	5538	0,53%
12	187.16.221.17	JuniperN_04:d7:f0	28287	Acer Telecomunicações LTDA	4808	0,46%
13	187.16.219.96	HuaweiTe_df:e2:12	52721	TOLEDO INFO LTDA	4709	0,45%
14	187.16.218.38	JuniperN_d5:d9:00	28209	Under	4392	0,42%
15	187.16.222.169	Routerbo_8e:bb:17	28244	SendNet Provider Ltda	4376	0,42%
17	187.16.221.171	Cisco_4b:22:c1	53065	OpçãoTelecom	4039	0,39%
18	187.16.218.106	JuniperN_d3:e8:02	26609	Universal Telecom S.A.	3975	0,38%
19	187.16.219.38	Routerbo_77:fb:3e	263055	Pinhais Telecom	3917	0,38%
21	187.16.217.8	Routerbo_3d:11:30	#N/D	#N/D	3736	0,36%
22	187.16.218.98	HuaweiTe_46:ec:0d	52551	SAMM Sociedade de Atividades em Mu	3698	0,36%
23	187.16.221.55	HuaweiTe_17:3a:39	262462	Aranet	3291	0,32%
26	187.16.219.217	JuniperN_c8:1f:c0	52579	NOROESTECOM	3117	0,30%
28	187.16.219.177	HuaweiTe_ee:bf:a0	262847	DEBUG	2964	0,28%
29	187.16.220.33	Routerbo_60:54:fe	#N/D	#N/D	2838	0,27%
30	187.16.220.11	JuniperN_55:d3:c0	262673	ViaReal Telecom	2834	0,27%
31	187.16.221.75	Routerbo_89:63:fb	262952	AIRLIFE COMUNICACAO VIRTUAL LTDA	2816	0,27%
32	187.16.218.236	Routerbo_f4:c5:2d	265347	BITAL TELECOM	2748	0,26%
35	187.16.217.163	JuniperN_f7:47:f0	#N/D	#N/D	2559	0,25%

Respondeu Request?			
Falha	%	Sucesso	%
12540	70,69%	5200	29,31%
13728	80,71%	3280	19,29%
6117	70,84%	2518	29,16%
6243	85,65%	1046	14,35%
3629	59,27%	2494	40,73%
3375	57,35%	2510	42,65%
4551	79,20%	1195	20,80%
4409	79,71%	1122	20,29%
3012	62,67%	1794	37,33%
3545	75,41%	1156	24,59%
2453	55,85%	1939	44,15%
3139	71,78%	1234	28,22%
2499	61,89%	1539	38,11%
2395	60,31%	1576	39,69%
2511	64,12%	1405	35,88%
2910	78,23%	810	21,77%
2058	55,70%	1637	44,30%
2380	72,38%	908	27,62%
1729	55,49%	1387	44,51%
2101	70,88%	863	29,12%
2119	74,72%	717	25,28%
2083	73,68%	744	26,32%
1964	69,82%	849	30,18%
1541	56,12%	1205	43,88%
1450	56,80%	1103	43,20%

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com

Como eu defini sucesso/falha na resposta de cada request?

- Criei uma nova pasta do Excel com a planilha dos pacotes coletados
- Ordenei os pacotes por Perguntado(Destino), Perguntador(Requisitante), e por Tempo.
- Criei uma coluna medindo o tempo entre os pacotes sequenciais.
- Criei uma coluna que determina sucesso ou falha dependendo do tempo entre os pacotes
- Se o **tempo entre dois ARP-Requests** do mesmo solicitante para o mesmo destino for **menor que 10 segundos** presumi que o pacote anterior não foi respondido (**Falha**).

No.	Time	Source	Perguntado	Perguntador	TempoEntrePkts	HouveFalha
90296	70.561.427	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	PrimeiroRequest	Falhou
91728	71.563.236	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,001809	Falhou
93130	72.565.307	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,002071	Respondeu
248936	193.706.667	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	121,14136	Falhou
251666	195.709.493	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	2,002826	Respondeu
409168	317.279.755	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	121,570262	Falhou
410614	318.281.647	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,001892	Falhou
412093	319.283.628	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,001981	Respondeu
563800	441.395.796	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	122,112168	Falhou
565077	442.397.755	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,001959	Respondeu
720411	563.641.963	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	121,244208	Falhou
722299	565.645.941	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	2,003978	Respondeu
876397	686.942.284	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	121,296343	Falhou
877756	687.944.188	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,001904	Falhou
879103	688.946.140	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,001952	Respondeu
1038831	810.027.493	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	121,081353	Falhou
1040195	811.028.351	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,000858	Falhou
1041589	812.030.351	IntelCor_89:01:6c	Who has 187.16.221.62	Tell 187.16.216.252	1,002	Respondeu

IX-SP - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
presumi que o pacote anterior não foi respondido (Falha).
fischerdouglass@gmail.com

Causas do ARP-Request Excessivo no IX-SP:

- Endereços IPs não atribuídos
 - Infraestrutura
 - ARP-Sponge (AMS-IX)
 - Honeypot
- Participantes com ARP-Timeout baixo
 - Origem
 - Default do Router-OS em 30s
- Shaping de ARP-Traffic para proteção das CPUs dos Routers
 - Destino
 - https://pt.wikipedia.org/wiki/Tragédia_dos_comuns

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

PeeringDB

IX.br (PTT.br) São Paulo

IPv4	187.16.216.0/21
IPv6	2001:12f8::/64

2046 hosts
que o
atual /21
permi

New Route

General Attributes

Dst. Address: 8.8.8.0/24

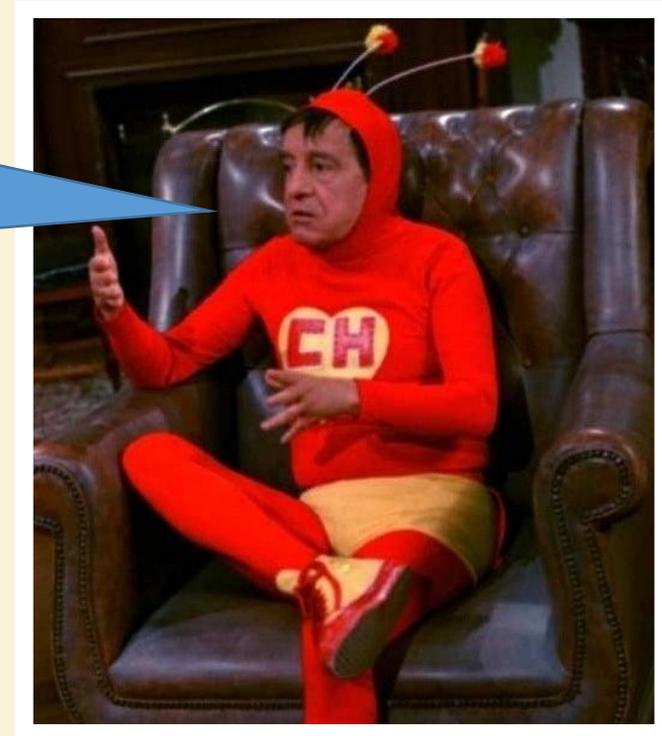
Gateway: 187.16.216.55

Check Gateway: ping

Type: unicast

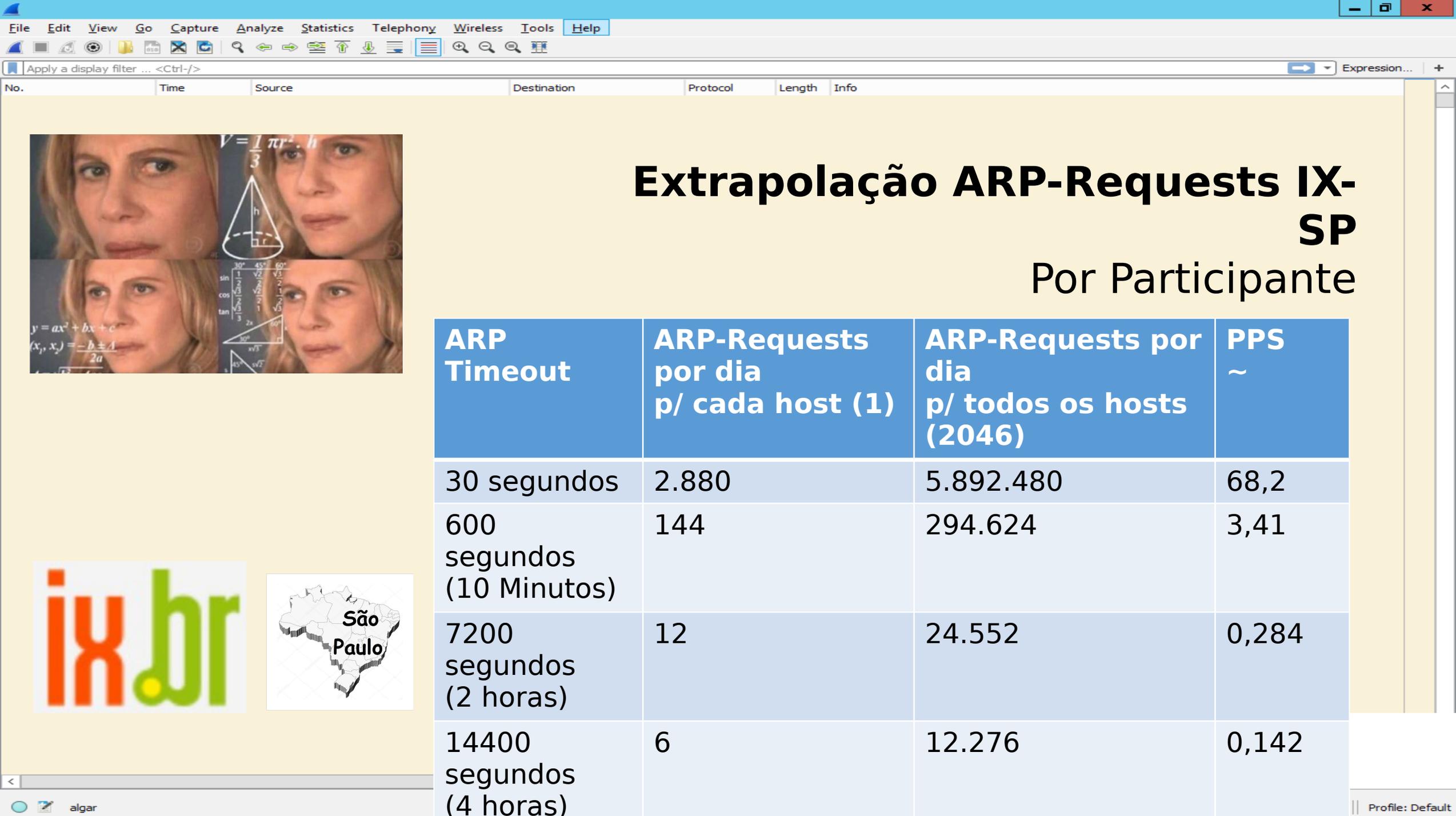
Todo mundo
fala
com todo
mundo

Tá, mas e como saber qual seria um bom número de PPS de ARP-Requests num barramento como o IX-SP?



Sem Shaping de
ARP

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglass@gmail.com



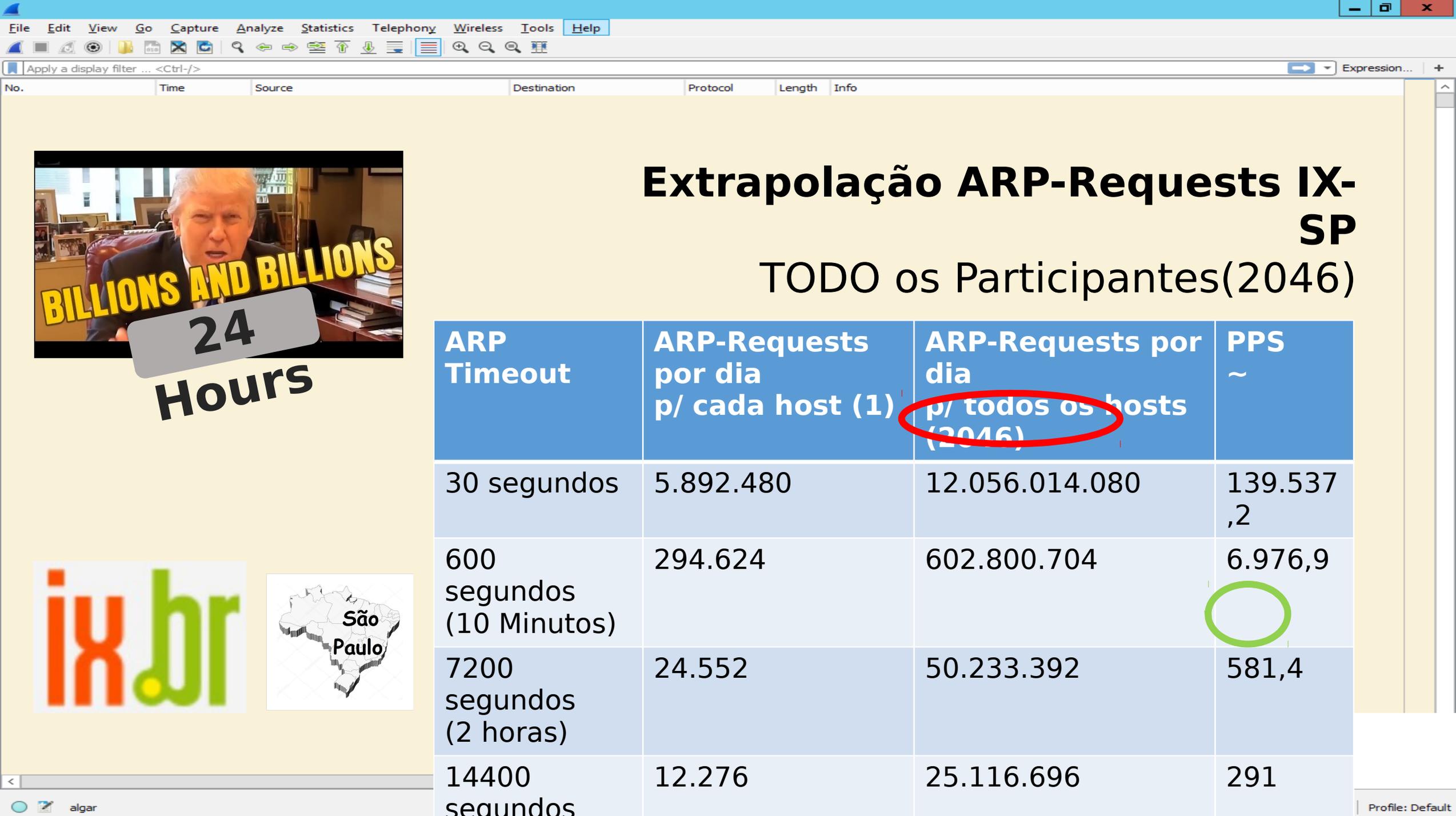
Extrapolação ARP-Requests IX-SP

Por Participante



ARP Timeout	ARP-Requests por dia p/ cada host (1)	ARP-Requests por dia p/ todos os hosts (2046)	PPS ~
30 segundos	2.880	5.892.480	68,2
600 segundos (10 Minutos)	144	294.624	3,41
7200 segundos (2 horas)	12	24.552	0,284
14400 segundos (4 horas)	6	12.276	0,142





Extrapolação ARP-Requests IX-SP

TODO os Participantes(2046)

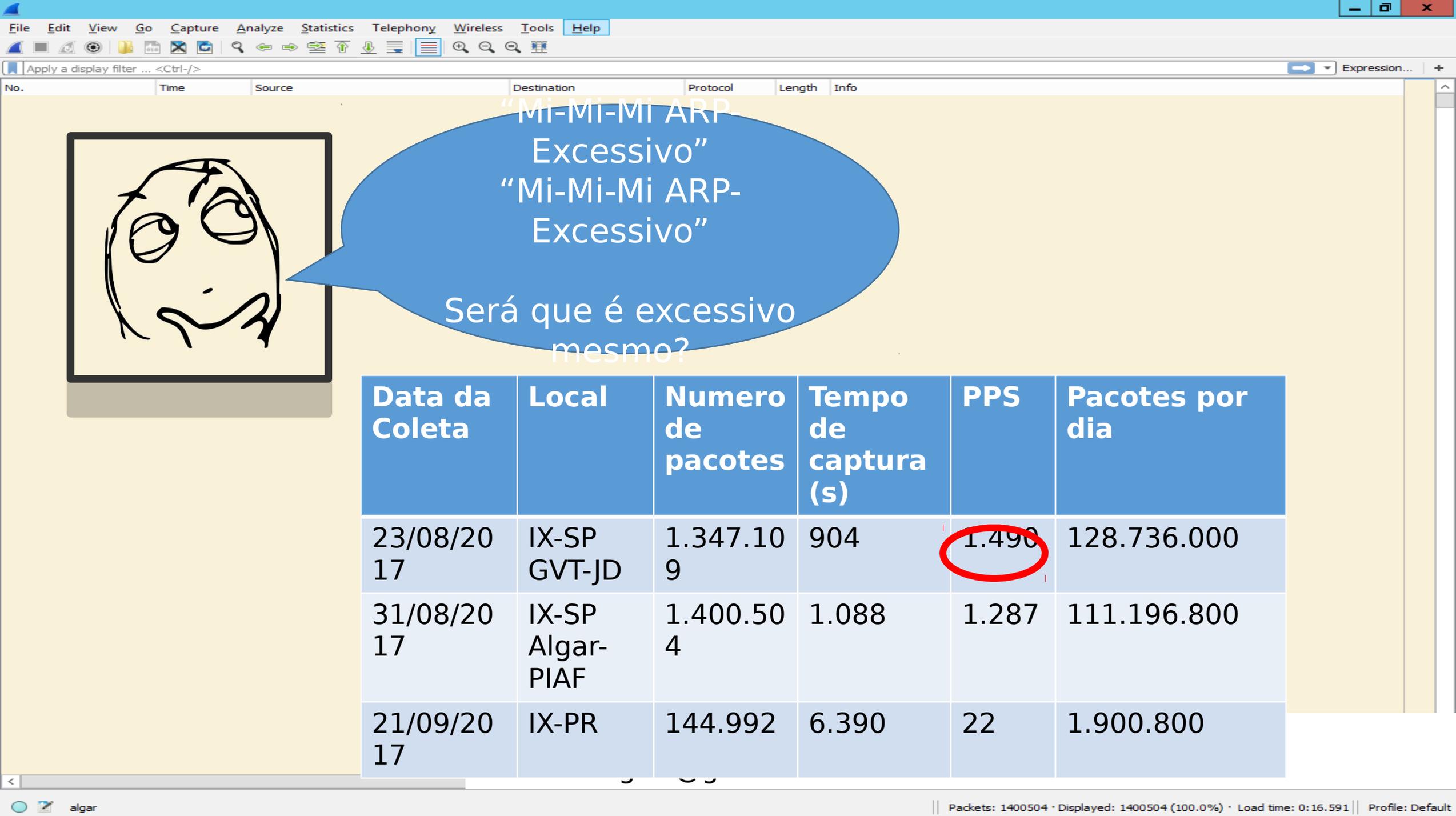
ARP Timeout	ARP-Requests por dia p/ cada host (1)	ARP-Requests por dia p/ todos os hosts (2046)	PPS ~
30 segundos	5.892.480	12.056.014.080	139.537,2
600 segundos (10 Minutos)	294.624	602.800.704	6.976,9
7200 segundos (2 horas)	24.552	50.233.392	581,4
14400 segundos	12.276	25.116.696	291



24 Hours



São Paulo



"MI-Mi-Mi ARP Excessivo"
"Mi-Mi-Mi ARP-Excessivo"

Será que é excessivo mesmo?

Data da Coleta	Local	Numero de pacotes	Tempo de captura (s)	PPS	Pacotes por dia
23/08/2017	IX-SP GVT-JD	1.347.109	904	1.490	128.736.000
31/08/2017	IX-SP Algar-PIAF	1.400.504	1.088	1.287	111.196.800
21/09/2017	IX-PR	144.992	6.390	22	1.900.800

Comparando os cenários

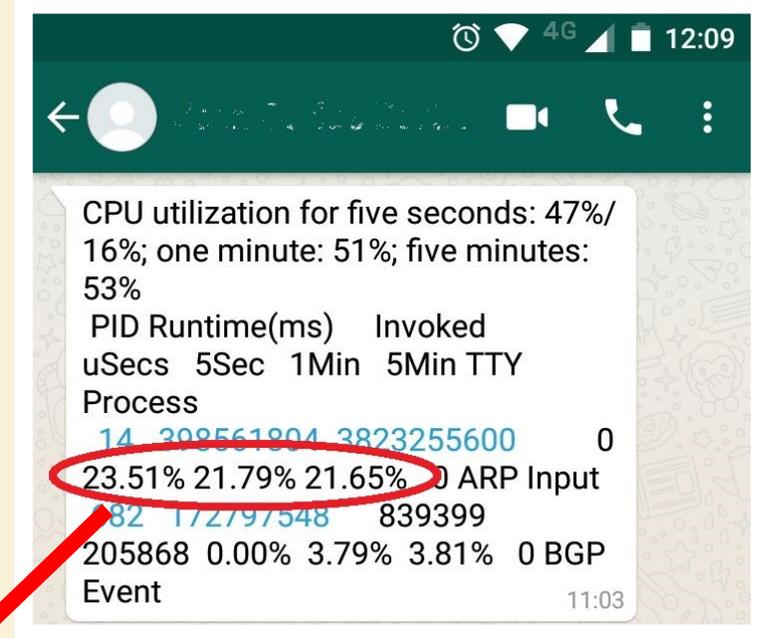
Coleta de 31/08/2017

- 1.287 PPS de ARP-Request
- 1270 Hosts

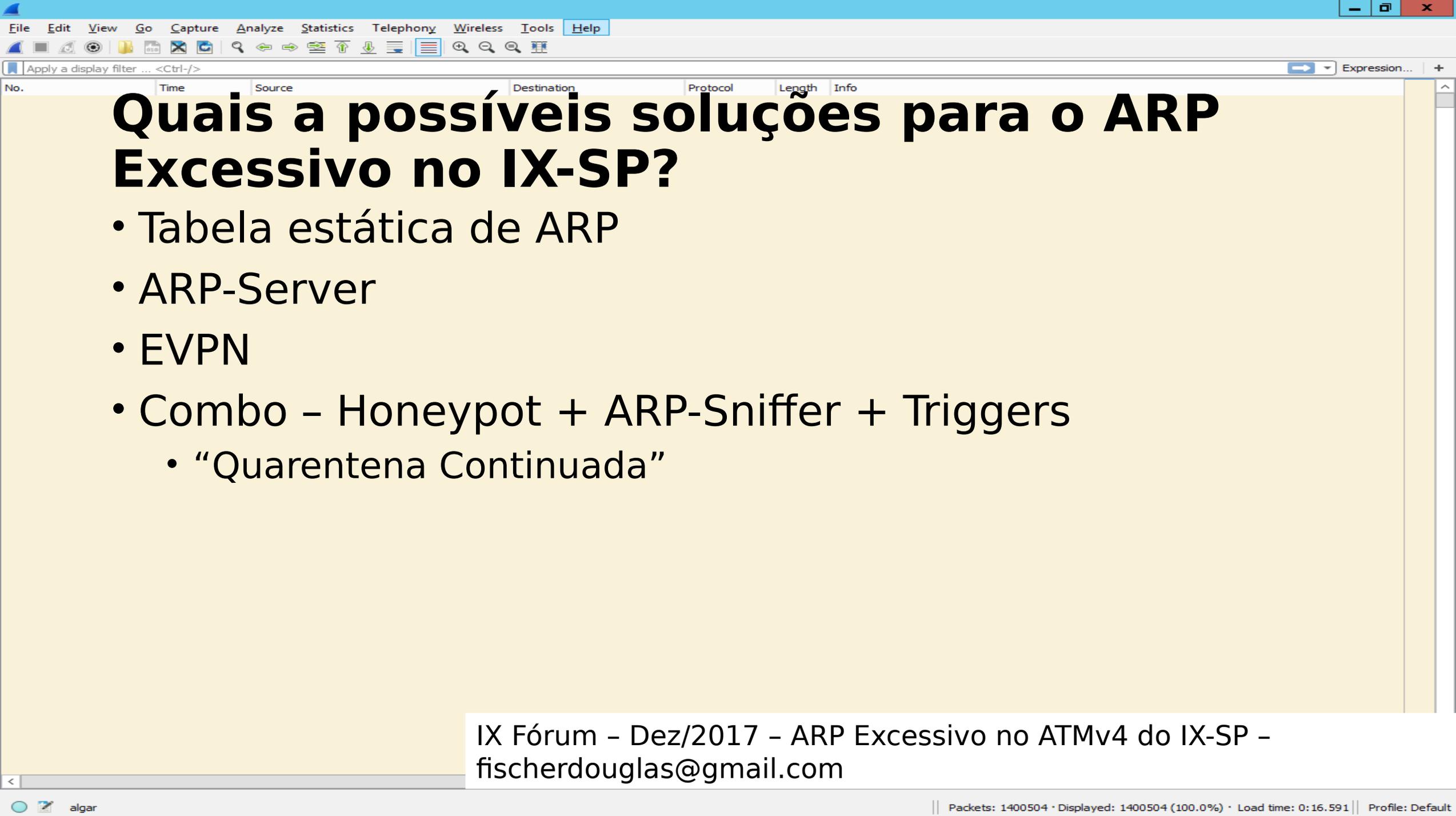
Cenário Hipotético ideal (4h)

- 291 PPS de ARP-Request
- 2046 Hosts

Redução de 4,42 X



4,89 %



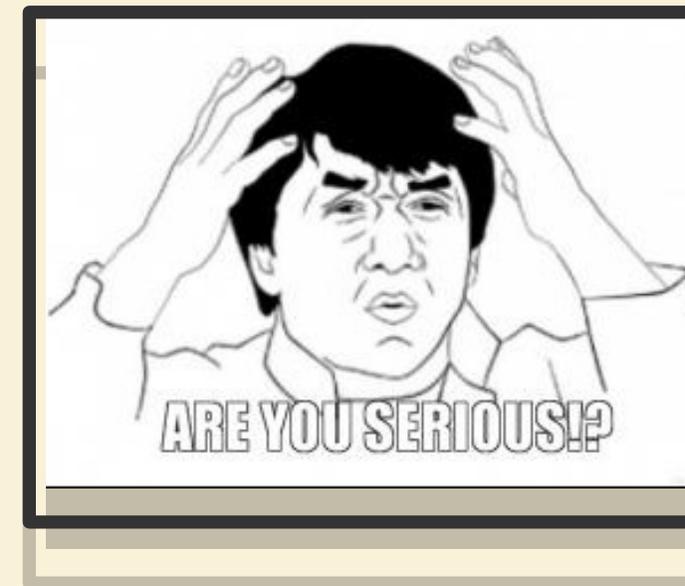
Quais as possíveis soluções para o ARP Excessivo no IX-SP?

- Tabela estática de ARP
- ARP-Server
- EVPN
- Combo - Honeypot + ARP-Sniffer + Triggers
 - “Quarentena Continuada”

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

Soluções ARP Excessivo IX - Tabela estática de ARP

- Cada participante deve configurar e manter MANUALMENTE os relacionamentos MAC <-> IP
 - Cisco(config)#arp 10.10.10.10 aaaa.aaaa.aaaa arpa
 - [admin@routerboard] > /ip arp add address=10.10.10.10 mac-address=AA:AA:AA:AA:AA:AA interface=ether1
- Susceptível a erros de operação
- Informação bastante dinâmica
 - +/- 1300 ajustes em 2016 em SP
- Teoricamente a tarefa poderia ser automatizada
 - Quem desenvolveria/customizaria a solução para cada plataforma?
- Custo inicial
 - Teoricamente baixo
- Custo operacional
 - Impossível mensurar(envolve participantes)



IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com

Soluções ARP Excessivo IX - ARP-Server

- Um(ou mais) Host rodando alguma engine de ARP-Server
 - Spoofing
 - Tabela Dinâmica ou Estática?
- Filtros de L2 de ARP-Request bloqueando os pacotes para Broadcast , deixando passar apenas para os ARP-Servers
 - Features de filtros de protocolo ARP nos Switchs do IX é pré-requisito (Outras Localidades?)
- Prós
 - Muito escalável
 - Simples
- Contras
 - Barulho não deixa de existir, apenas está contido
 - Maquia o verdadeiro status L2 dos hosts(Checkgateway)
 - Ponto Único de Falha (Response-delay)
- Custo inicial
 - Desenvolvimento/implementação da solução
 - Configuração de filtros e toda malha do IX-SP
- Custo operacional
 - Manutenção dos ARP-Servers
 - Manutenção dos filtros de ARP m



IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

Soluções ARP Excessivo IX - EVPN

- Equipamento ativo em cada PIX que fará a supressão de ARP
- Prós
 - Robusto
 - Escalável
- Contras
 - Cria possíveis amarras a fabricantes - Interoperabilidade
 - Barulho não deixa de existir, apenas está contido
 - Maquia o verdadeiro status L2 dos hosts(Checkgateway)
- Custo inicial
 - Aquisição dos Equipamentos(ou licenças)
 - Migração de ambiente
- Custo operacional
 - Manutenção dos PEs
- Outras features também estão no EVPN
 - Supressão de ARP é só uma delas (Vem de lambuja)
- Sem redução relativa de custos ao replicar a solução em outras localidades



IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

Soluções ARP Excessivo IX - Combo Mágico

- Honeypot
- ARP-Sniffer - Triggers - Ações - Workflow
- Sem pontos de falha que causem inoperância
 - Passivo em relação a operação do protocolo ARP em si
 - Depois de várias iterações tornará o ambiente estável
 - "Quando um gerente faz bem o seu trabalho, sua intervenção acaba se tornando desnecessária."
- Custo inicial
 - Definição das políticas e penalidades
 - Desenvolvimento e implantação das soluções
- Custo operacional
 - Manutenção dos serviços
 - Operação automatizada
- Baixo custo de replicação da solução nas demais localidades
 - Quiçá outros IX!?!?! (Op IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP - fischerdouglas@gmail.com



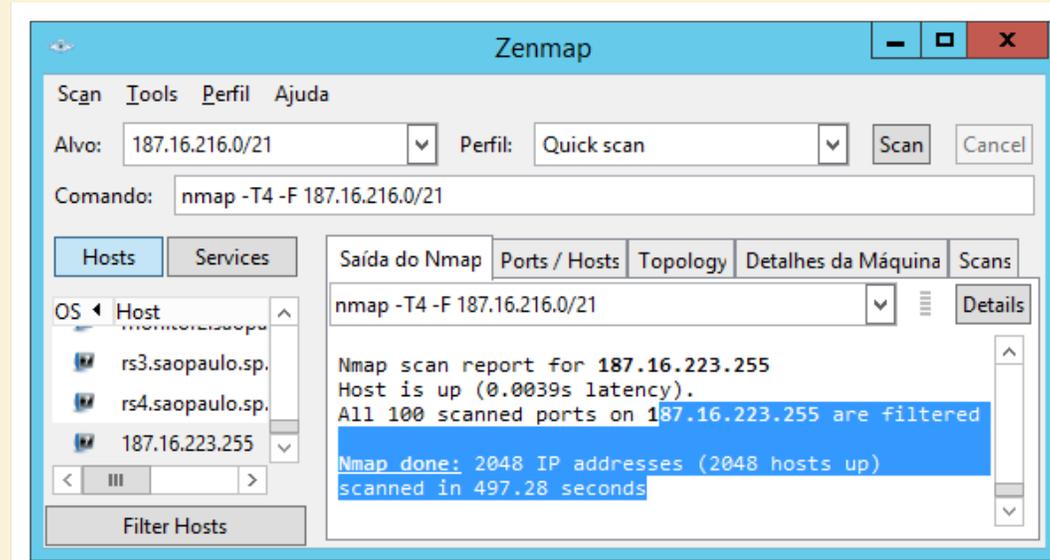
Combo Mágico - Honeypot

- IX-SPO 2046 IPs Disponíveis, Atualmente +/- 1300 hosts, 700 IPs “vagos”
- Host com múltiplos IPs secundários definidos automaticamente
 - Algum sistema automatizado consulta ciclicamente os sistemas do IX.BR e define os IPs não atribuídos daquela localidade
 - Algum Mecanismo de Orquestração provisiona esse Honeypot com todos esses IPs
- Além de ARP, esse host não responderia a “nada”
 - Talvez ICMP?
- Possibilidade de uso das informações no combate a DoS e outras técnicas maliciosas
 - Varreduras pode ser um bom indicativo de iminentes DoSs
 - ?? Criatividade ??



Apenas Ideias!
E ainda estão
em
< Release Pré-

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com



Combo Mágico - ARP-Sniffer

- Host sniffando a rede
 - Contabilizando e registrando minuto-a-minuto (Timeslots):
 - Pacotes de ARP-Request que <EsseHost> emitiu contra os demais participantes (2046 sensores)
 - Pacotes de ARP-Request foram emitidos contra <EsseHost> (2046 sensores)
 - “Re-Pergunta” - Falha? (4,1Milhões de sensores)
 - Fazendo Log de:
 - Gratuitous-ARP
 - ARP-Requests perguntando destino fora da faixa de rede local
 - ARP-Requests com o “Tell” fora da faixa de rede local



Apenas Ideias!
E ainda estão
em
< Release Pré-

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com

Combo Mágico - Triggers

- Tolerâncias
 - Rajadas Verdadeiras
 - Falhas de conectividade do Participante/Transporte
 - Falhas nos Route-Servers
 - Falhas em algum PIX específico ou até generalizada
 - Coincidência temporal de Expiração de ARP-Entries
 - 4 horas depois de um Up/Down de Interface
 - 4 horas depois da convergência de rotas(Checkgateway)

• Métrica de análise de conformidade

- ARP-Requests emitidos pelo participante
 - 1 ou mais Timeslots excedidos últimos 10 minutos = 1 Strike
 - 3 ou mais Strikes na ultima uma hora = 1 Pên
- ARP-Requests emitidos contra o participante
 - Indicar Shaping a

25 PPM?

**ARP-Requests
1 host
ARP-Timeout de 4h
Contra 2046
hosts(/21)**

Pacotes por Segundo	0,14 2
---------------------	-----------

Pacotes por Minuto	8,52 5
---------------------------	-------------------

Pacotes por 5 minutos	42,6 5
-----------------------	-----------

Pacotes por Hora	511,
------------------	------



Apenas Ideias!
E ainda estão em
em
< Release Pré-

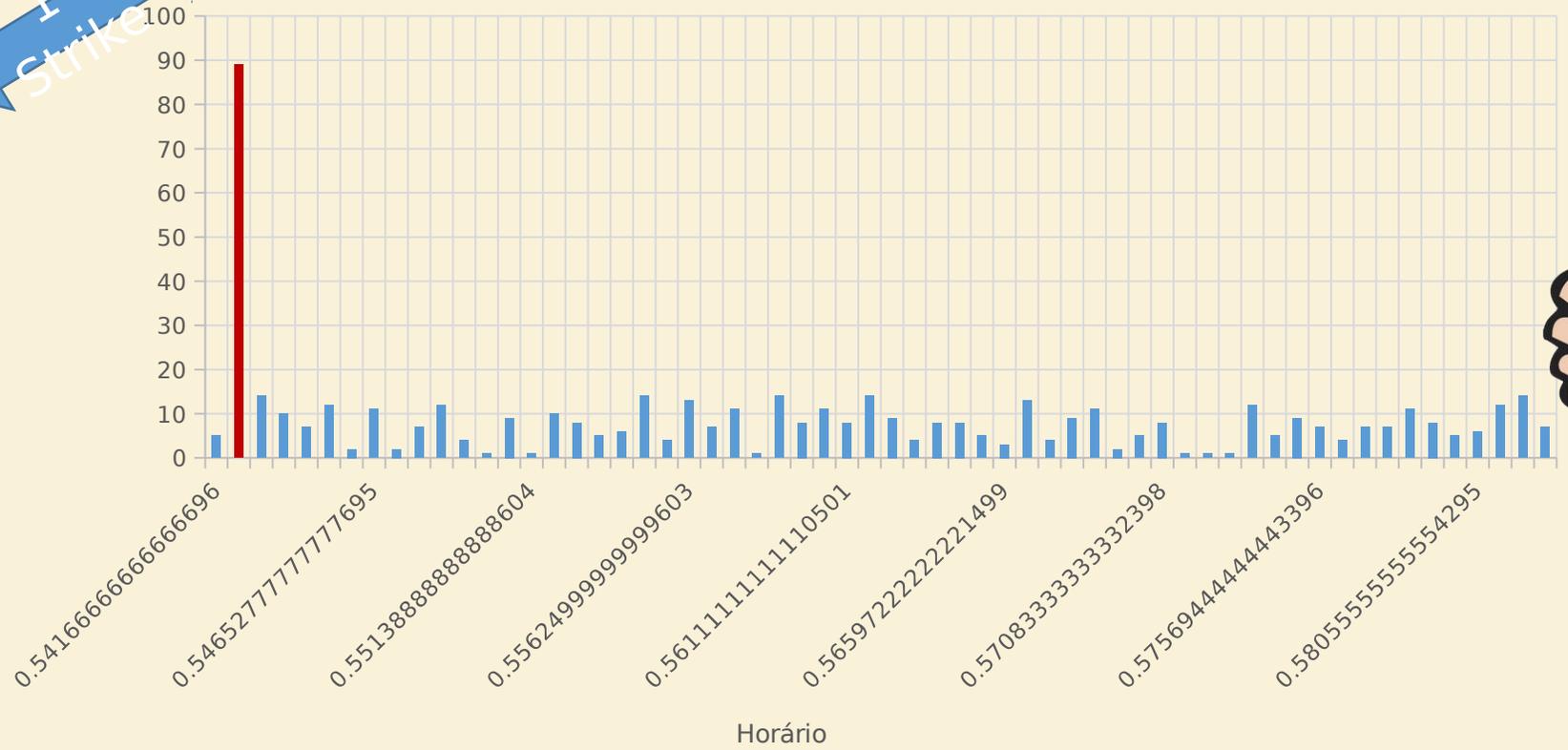
IX Fórum - Dez/2017 - ARP Excessivo r
fischerdouglas@gmail.com

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

ARP-Requests - Um participante - Ideal

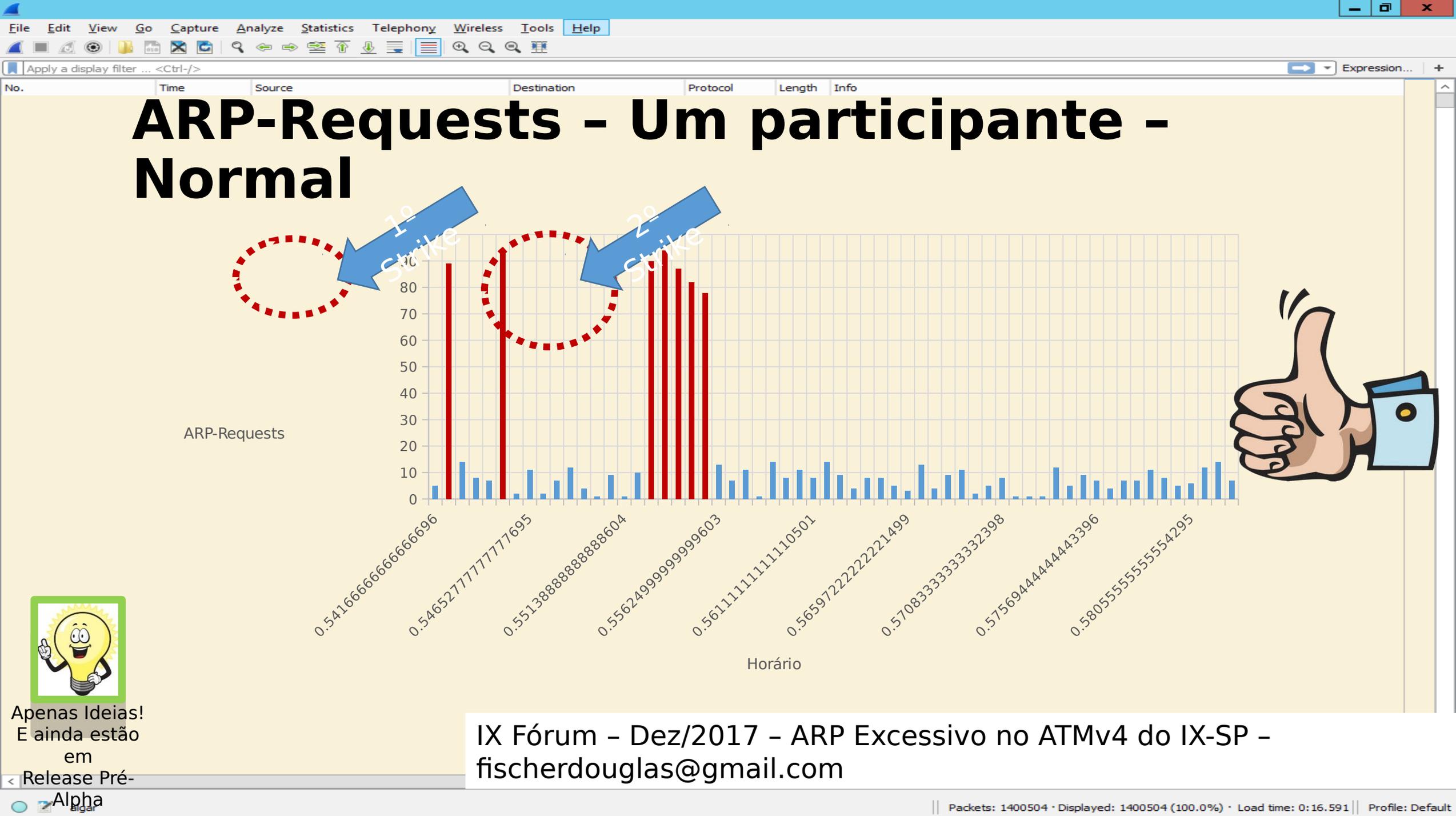


ARP-Requests



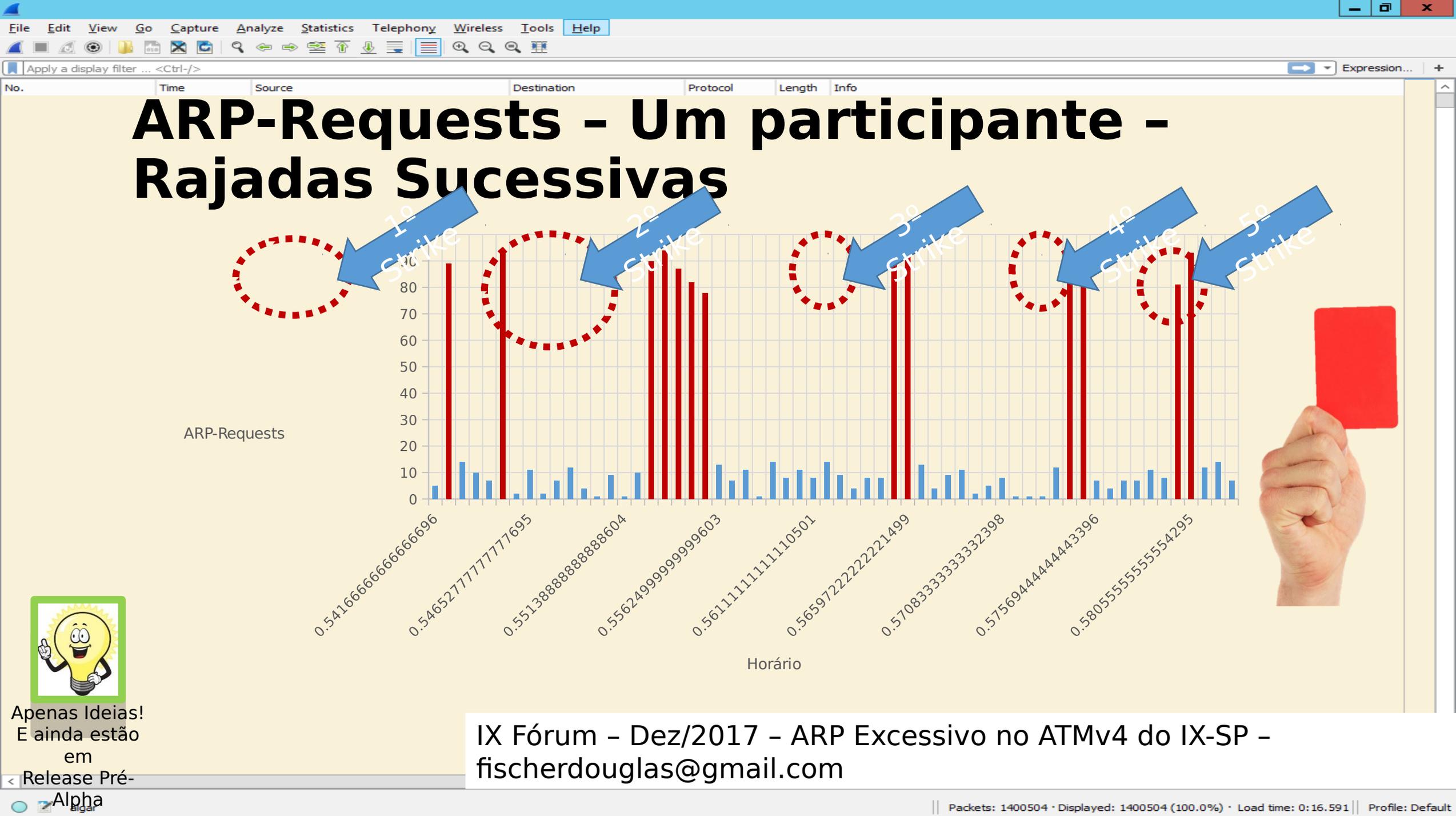
Apenas Ideias!
E ainda estão
em
Release Pré-

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com



Apenas Ideias!
E ainda estão
em
Release Pré-

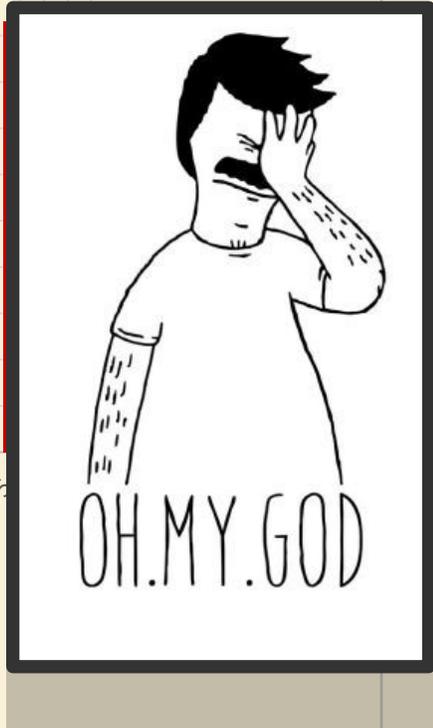
IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com



Apenas Ideias!
E ainda estão
em
Release Pré-

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com

ARP-Requests - Um participante - Excessivo



Apenas Ideias!
E ainda estão
em
Release Pré-
Alpha

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com

Combo Mágico - Ações

- Notificação automatizada aos responsáveis pelo host que gerou não conformidade
 - Prazo de X horas comerciais(SPO) para correção do problema
- Gratuitous-ARP of Death
 - Host específico emitirá rajadas de ARP-Gratuito com um Mac-Address falso
- API (ou Ansible) - Route-Servers
 - Clear na sessão BGP do host que gerou o problema
 - Shutdown na sessão BGP do host que gerou o problema
- API - SDN
 - E as localidades do IX.BR com Switch que não suportam SDN?
 - Mudar a Vlan-Translation para uma Vlan de Quarentena
- Hall of Shame - Idea congelada

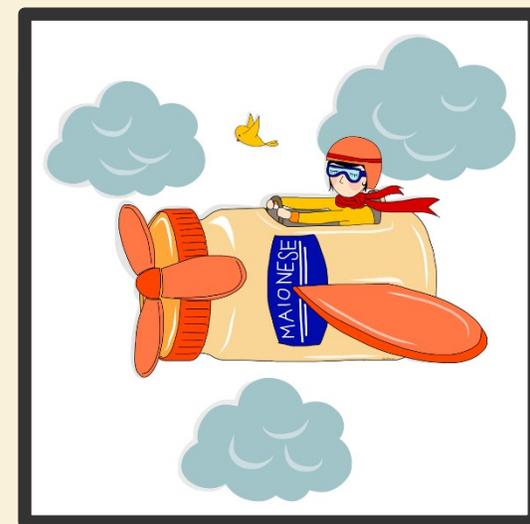
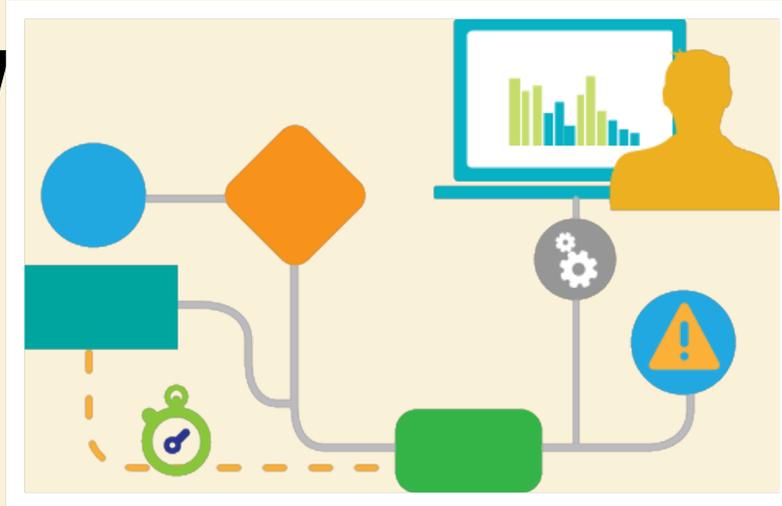


Apenas Ideias!
E ainda estão
em
< Release Pré-

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com

Combo Mágico - WorkFlow

- Não conformidade identificada?
 - ARP Excessivo / Shapping abusivo / ARP Gratuito / Etc
- 1ª ocorrência nas últimas 50 horas comerciais?
 - Notificação por e-mail
 - 10 horas comerciais de São Paulo(ou localidade)
- 2ª ou 3ª ocorrências nas últimas 50 horas comerciais?
 - Clear nas sessões dos Route-Servers + e-mail
 - 10 horas comerciais de São Paulo(ou localidade)
- 4ª ou 5ª ocorrências nas últimas 50 horas comerciais?
 - Arp Gratuito da Morte + e-mail
 - 10 horas comerciais de São Paulo(ou localidade)
- 6ª ocorrência nas últimas 50 horas comerciais?
 - Shutdown nas sessões dos Route-Servers + e-mail
 - Só reestabelece abrindo chamado no Meu.IX



Apenas Ideias!
E ainda estão
em
< Release Pré-

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglas@gmail.com

Locais de troca de informação sobre IX.BR

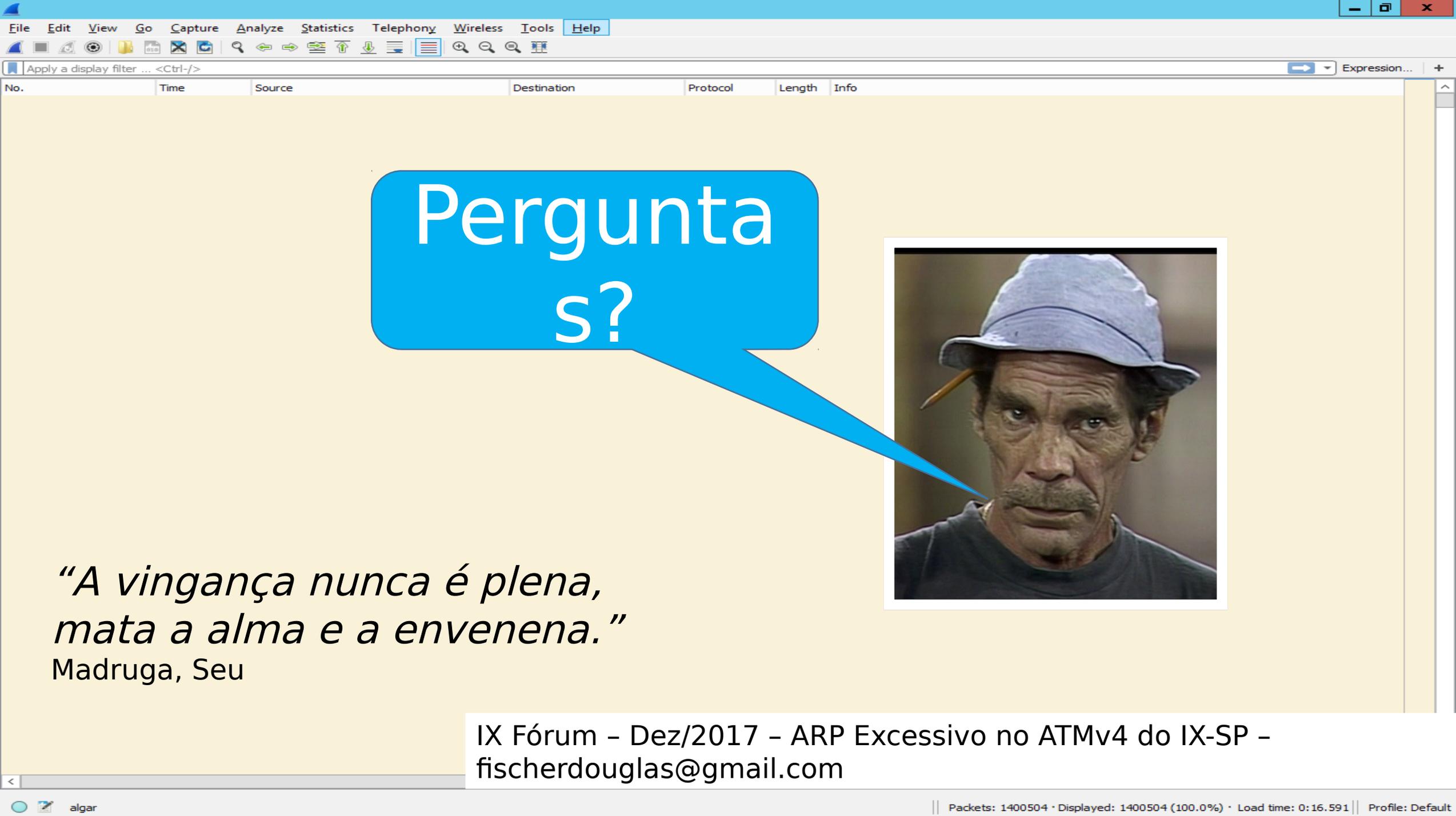
http://t.me/ix_br_usuarios



<https://eng.registro.br/mailman/listinfo>

List	Description
Anuncios-dnssec	Lista de Anuncios - KSK rollover .br
caiu	Lista das indisponibilidades da Internet brasileira
CP-GTS	Comite de programa do GTS
DNSSHIM	DNS Secure Hidden Master
eppnicbr	EPP no .br - protocolo e operacao
gter	Grupo de Trabalho de Engenharia e Operacao de Redes
GTS-L	Grupo de Trabalho em Segurança de Redes
Inoc-br	InterNOC DialByAsn Brasil
masoch-l	Mail Aid and Succor, On-line Comfort and Help
openflow	Lista eletrônica sobre Openflow e SDN (Software Defined Networks)
spam-l	Spam-l

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com



Perguntas?



*“A vingança nunca é plena,
mata a alma e a envenena.”*

Madruga, Seu

IX Fórum - Dez/2017 - ARP Excessivo no ATMv4 do IX-SP -
fischerdouglass@gmail.com