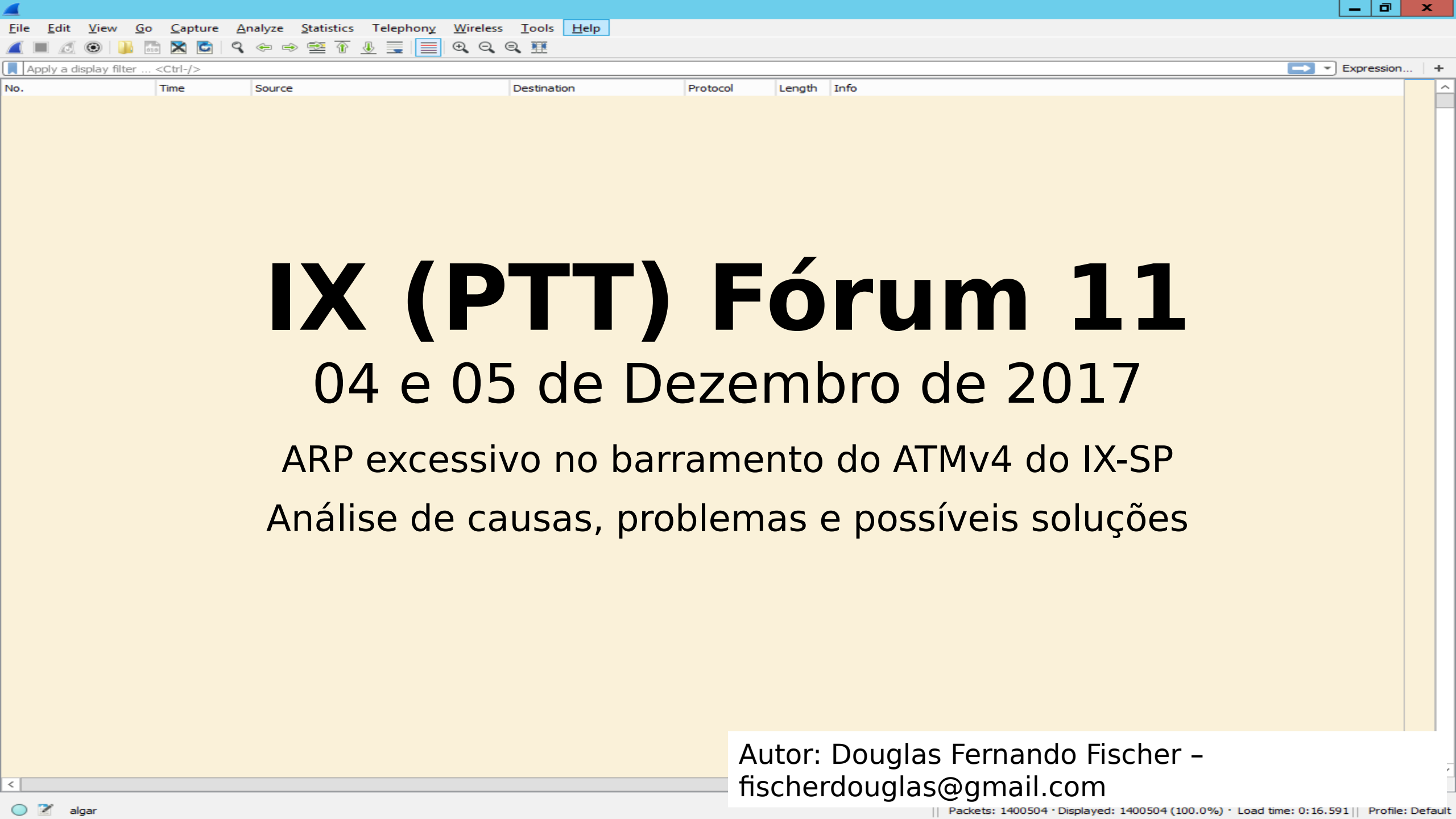


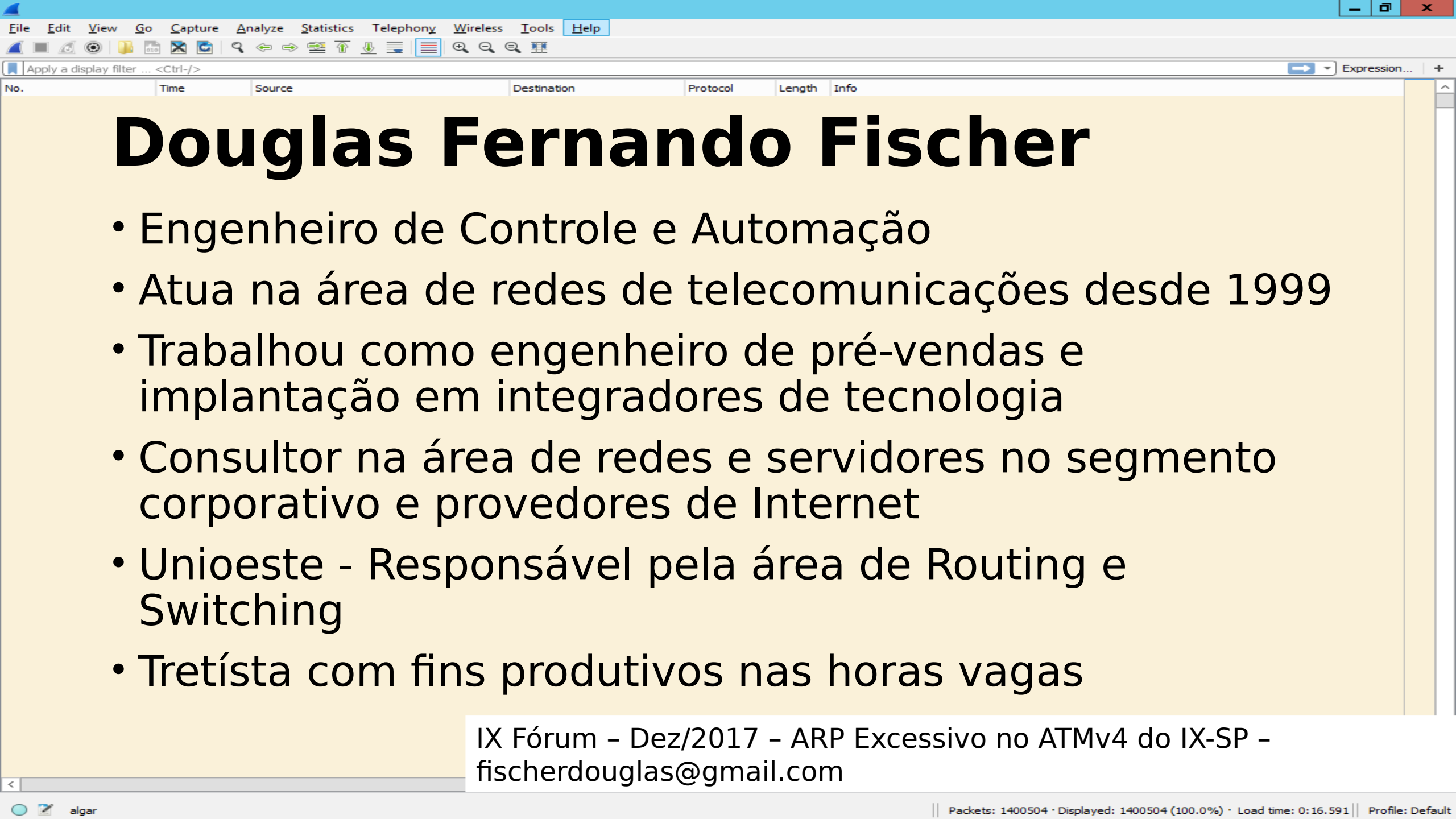
IX (PTT) Fórum 11

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No. Time Source Destination Protocol Length Info

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 GRAAANDE 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

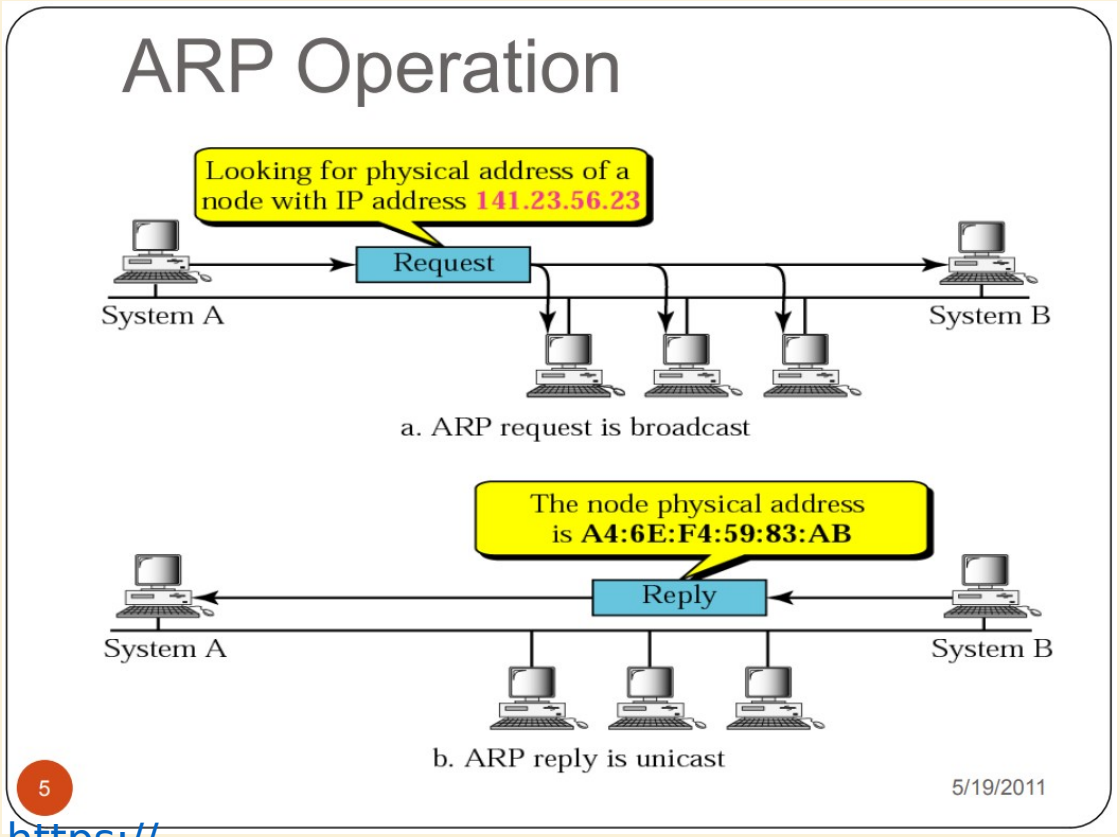
algar Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 Profile: Default

ARP – Address Resolution Protocol

tps://tools.ietf.org/html/rfc826 (1982)

É a “coisa grudenta” que junta:

Endereços físicos	⇔	Endereços lógicos
Mac-Address		IP-Address
Layer 2		Layer 3

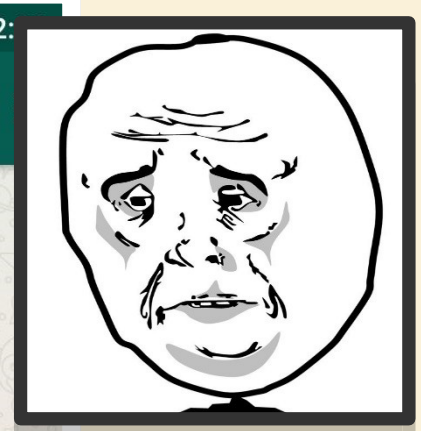


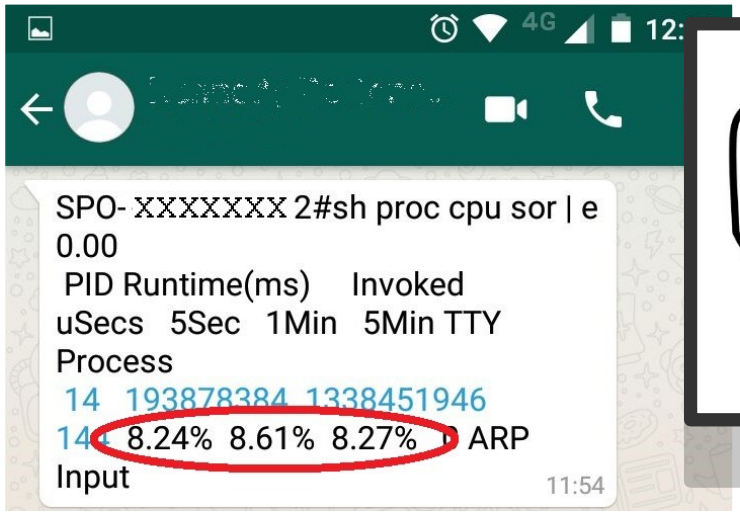
https://pt.slideshare.net/tigerbt/arp-address-resolution-protocol

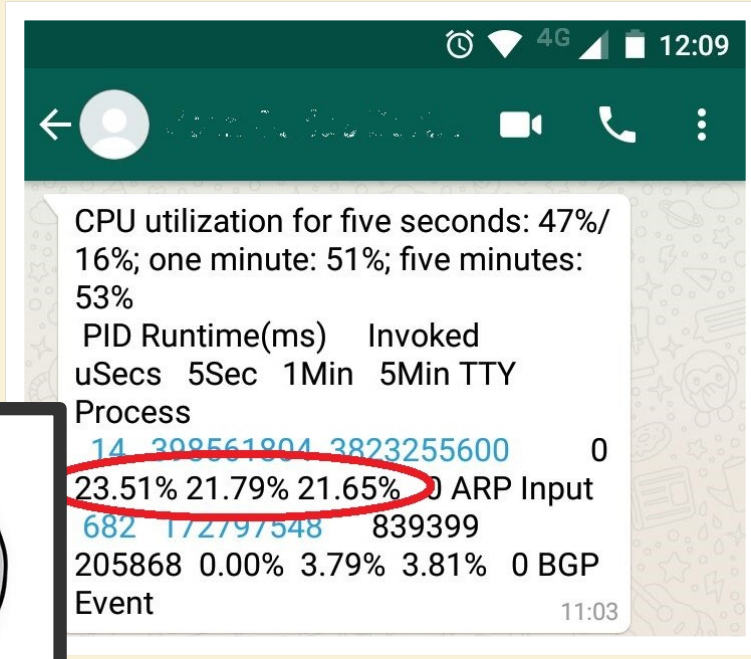
https://pt.wikipedia.org/wiki/ARP

Como essa encrenca caiu no meu colo?

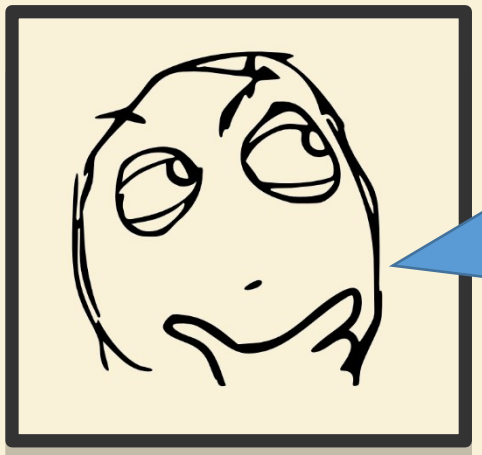
Software-based vs Hardware-based Routers







IX Fórum – Dez/2017 – ARP Excessivo no ATMv4 do IX-SP – fischerdouglas@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 escutamos falar sobre problemas com ARP no PTT-SPO.

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

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

Paulo Henrique paulohenriquef@gmail.com por eng.registro.b 20/03/2013

para Grupo

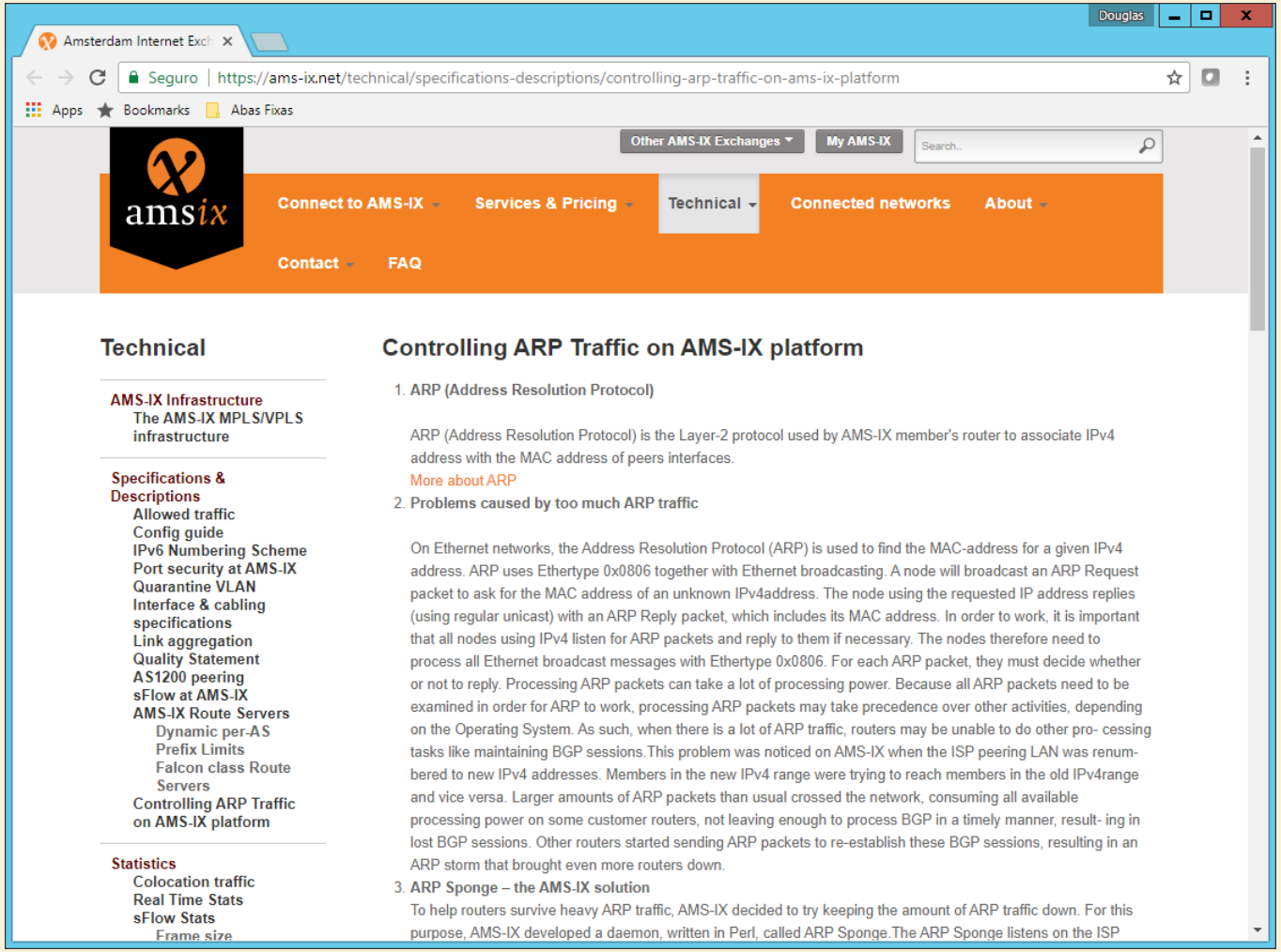
Pessoal, como o assunto acabou voltando a ser levantado na lista e eu ainda não havia postado nada até hoje, resolvi então escrever para relatar nossa situação atual.
Depois de muitas buscas acabei me deparando com este material do Amsterdam Internet Exchange:

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

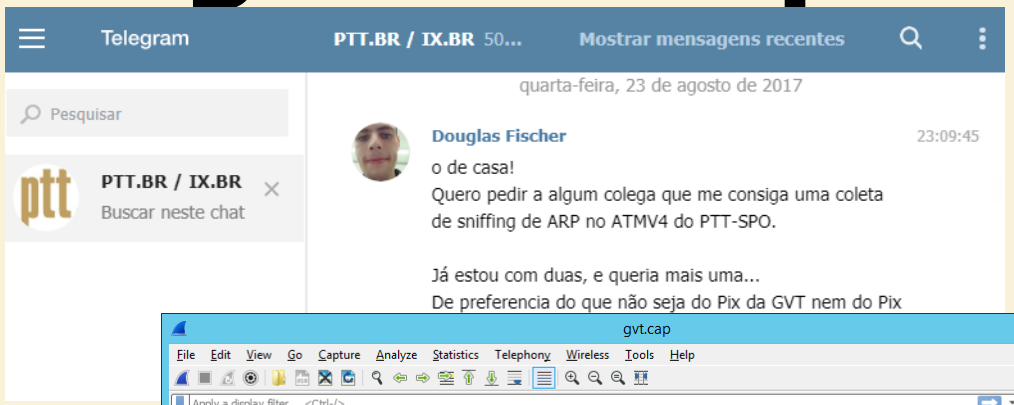
Como eu havia dito, utilizamos linux como roteador, então, fiz as seguintes configurações:

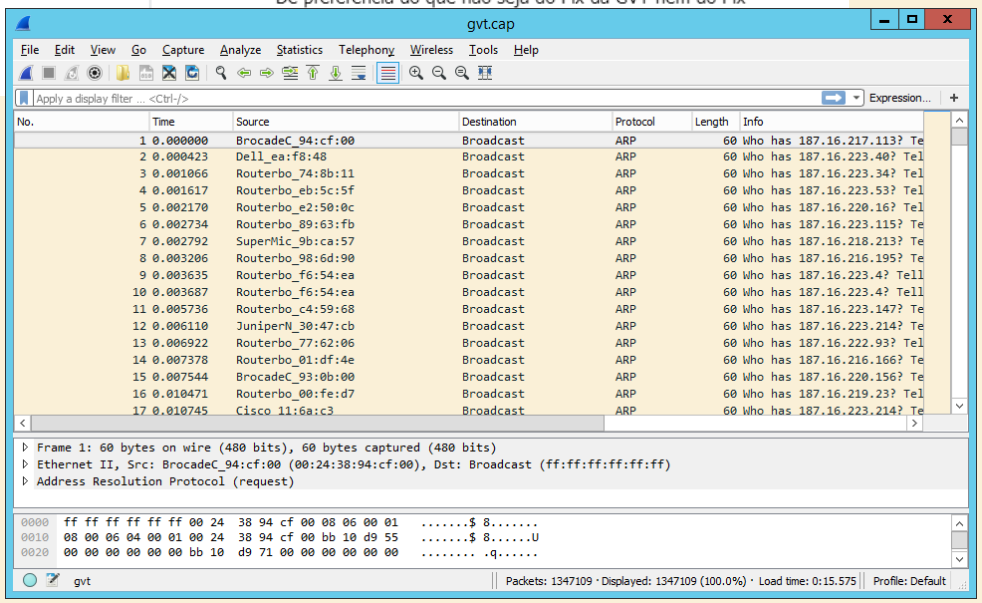
net.ipv4.neigh.IF_XXX.base_reachable_time = 14400
net.ipv4.neigh.IF_XXX.gc_stale_time = 1200

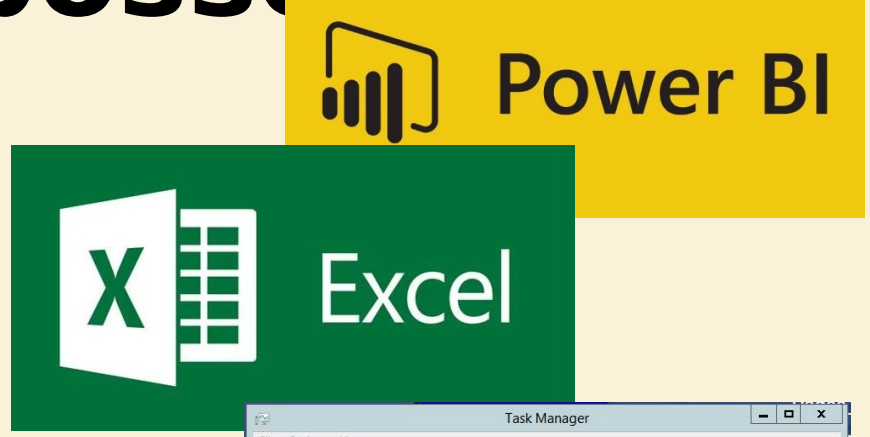
Também não somos os primeiros do mundo a sofrer com isso.

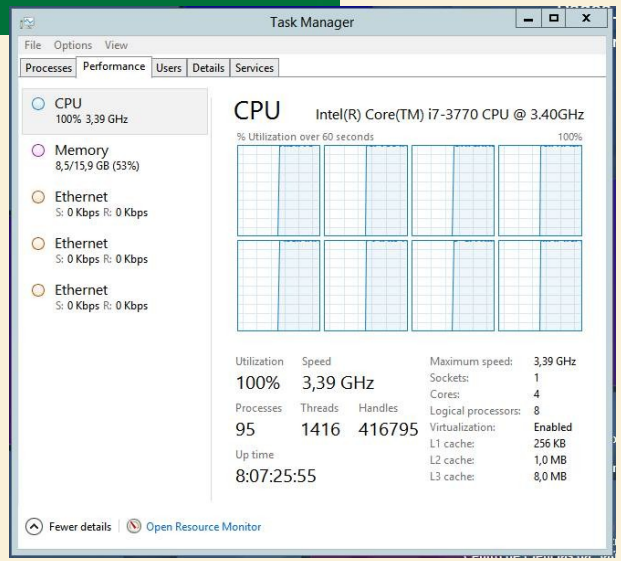


E agora? O que eu posso fazer?









algar

Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 Profile: Default

Primeiras Análises (23/08/2017)

Análise dos pacotes de Brodcasts transmitidos no IX-SP

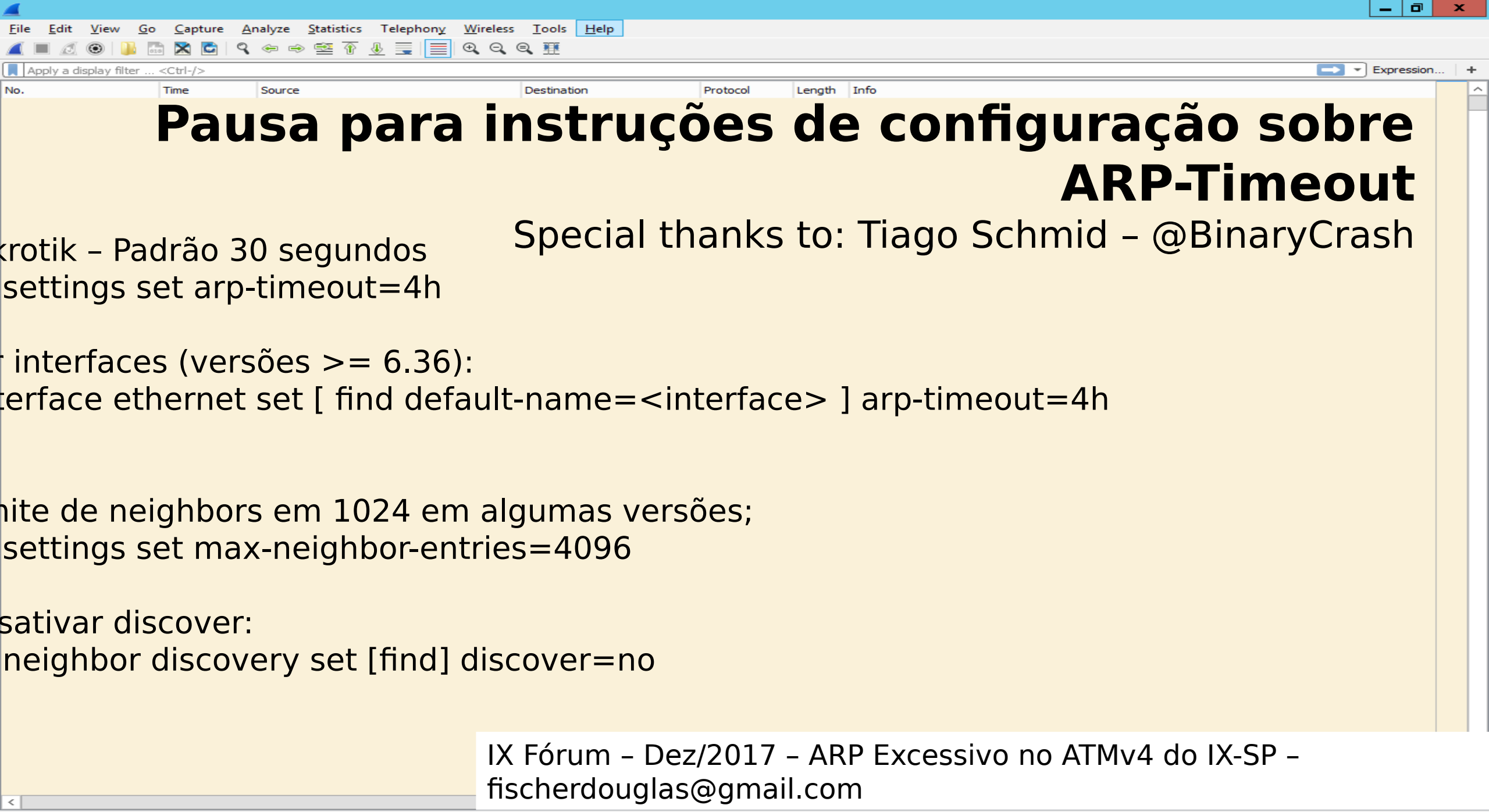
Capturas realizadas em multiplos PIX em 23/08/2017

Fabricante	% requests Emitidos
Routerbo	56,25%
JuniperN	12,70%
Dell	5,99%
IntelCor	5,87%
Cisco	5,54%
Ubiquiti	3,15%
BrocadeC	2,01%
Broadcom	1,75%
Serveru	1,29%
Vmware	0,81%
Ibm	0,62%
AristaNe	0,55%
SuperMic	0,49%
HuaweiTe	0,45%
AxiomTec	0,44%

Fabricante	% requests procurados
Routerbo	30,15%
(vazio)	21,00%
JuniperN	16,76%
HuaweiTe	10,14%
Cisco	8,64%
IntelCor	3,39%
Serveru	1,93%
Ubiquiti	1,87%
Dell	1,30%
HewlettP	0,57%
SuperMic	0,55%
ChelsioC	0,41%
LannerEl	0,40%
Vmware	0,39%
BrocadeC	0,35%

Fabricante	Qtde. part. por EUI	% Relativo
Routerbo	624	44,86%
JuniperN	267	19,19%
Cisco	92	6,61%
IntelCor	81	5,82%
Ubiquiti	50	3,59%
Dell	44	3,16%
HuaweiTe	39	2,80%
Serveru	29	2,08%
Broadcom	23	1,65%
Trendnet	22	1,58%
Ibm	16	1,15%
HewlettP	12	0,86%
BrocadeC	12	0,86%
LannerEl	11	0,79%
SuperMic	9	0,65%

https://drive.google.com/file/d/0B2ezlM5MIr8PbE9LbE1TRmRuaUU/view



Pausa para instruções de configuração sobre ARP-Timeout

Special thanks to: Tiago Schmid – @BinaryCrash

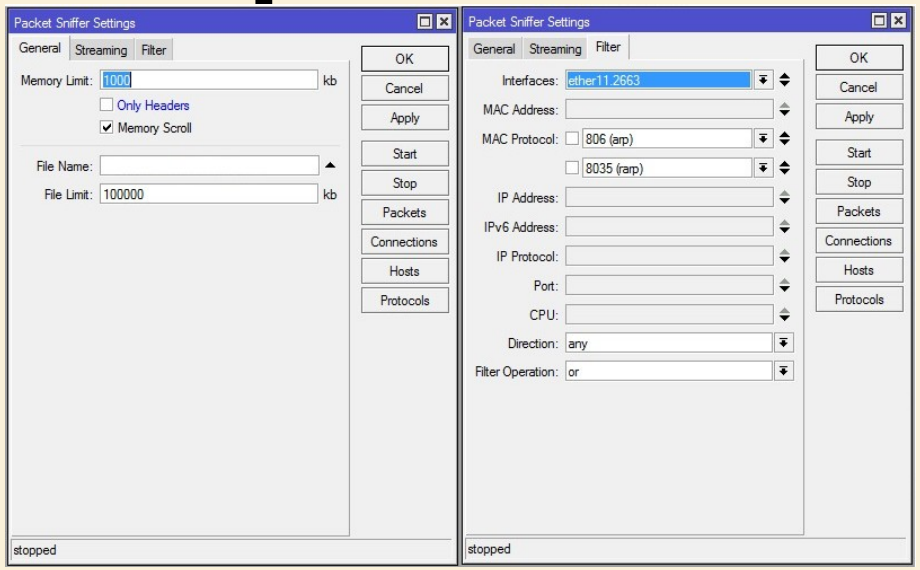
krotik – Padrão 30 segundos
settings set arp-timeout=4h

interfaces (versões >= 6.36):
terface ethernet set [find default-name=<interface>] arp-timeout=4h

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

sativar discover:
neighbor discovery set [find] discover=no

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

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

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

Douglas Fischer fischerdouglas at 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

Seguem os links para os arquivos:

SniffingARP-IX-SP_2017-08-31_ConfiguraçõesIncoerentes.pdf
https://drive.google.com/open?id=0B2ezlM5MIr8PVGViY3JSc0xMX1E

SniffingARP-IX-SP_2017-08-31_ResumoPorFabricante.pdf
https://drive.google.com/open?id=0B2ezlM5MIr8PenBHN18yWDNtdnc

SniffingARP-IX-SP_2017-08-31_ResumoPorIPProcurado.pdf
https://drive.google.com/open?id=0B2ezlM5MIr8PUjZPOEJzM3NGMEE

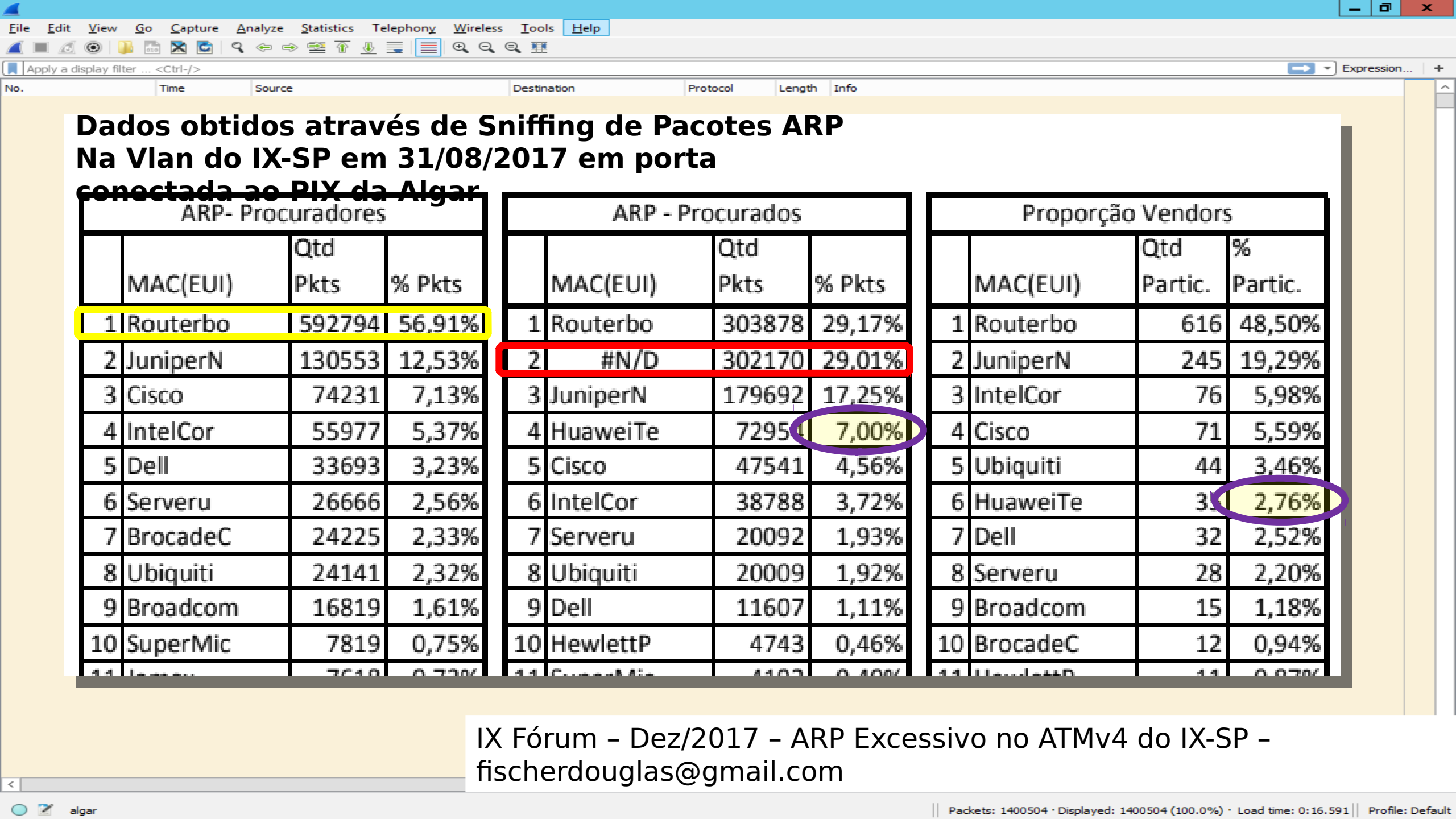
SniffingARP-IX-SP_2017-08-31_ResumoPorIPProcurador.pdf
https://drive.google.com/open?id=0B2ezlM5MIr8PNjJPTXNfUmlxLTg

SniffingARP-IX-SP_2017-08-31_SemDadosDaColeta.xlsx (631KB)
https://drive.google.com/open?id=0B2ezlM5MIr8PT01nUDRzVTBmWDA

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

IX Fórum – De
fischerdouglas

algar



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

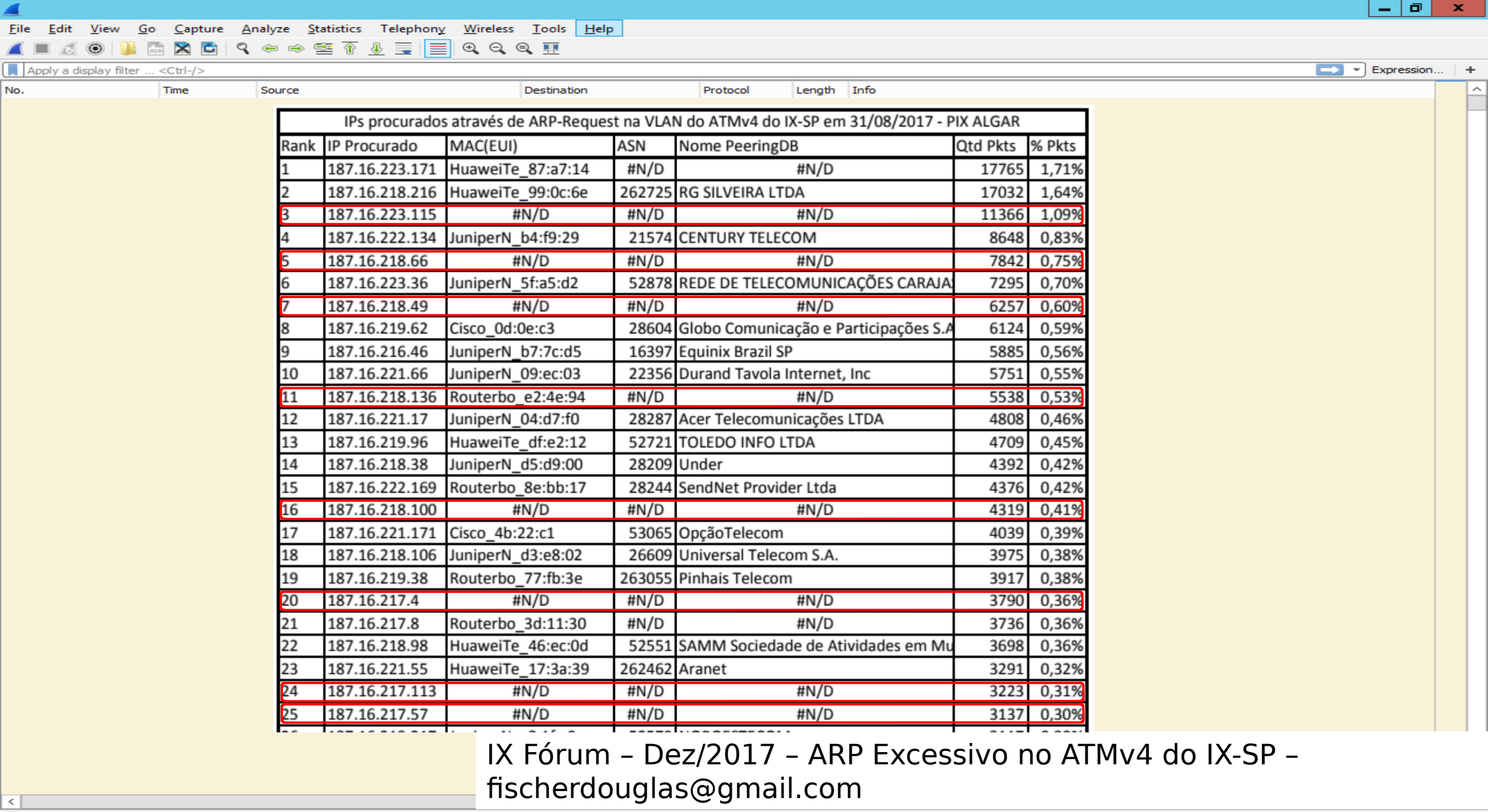
	MAC(EUI)	Qtd Pkts	% Pkts
1	Routerbo	592794	56,91%
2	JuniperN	130553	12,53%
3	Cisco	74231	7,13%
4	IntelCor	55977	5,37%
5	Dell	33693	3,23%
6	Serveru	26666	2,56%
7	BrocadeC	24225	2,33%
8	Ubiquiti	24141	2,32%
9	Broadcom	16819	1,61%
10	SuperMic	7819	0,75%

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	7295	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

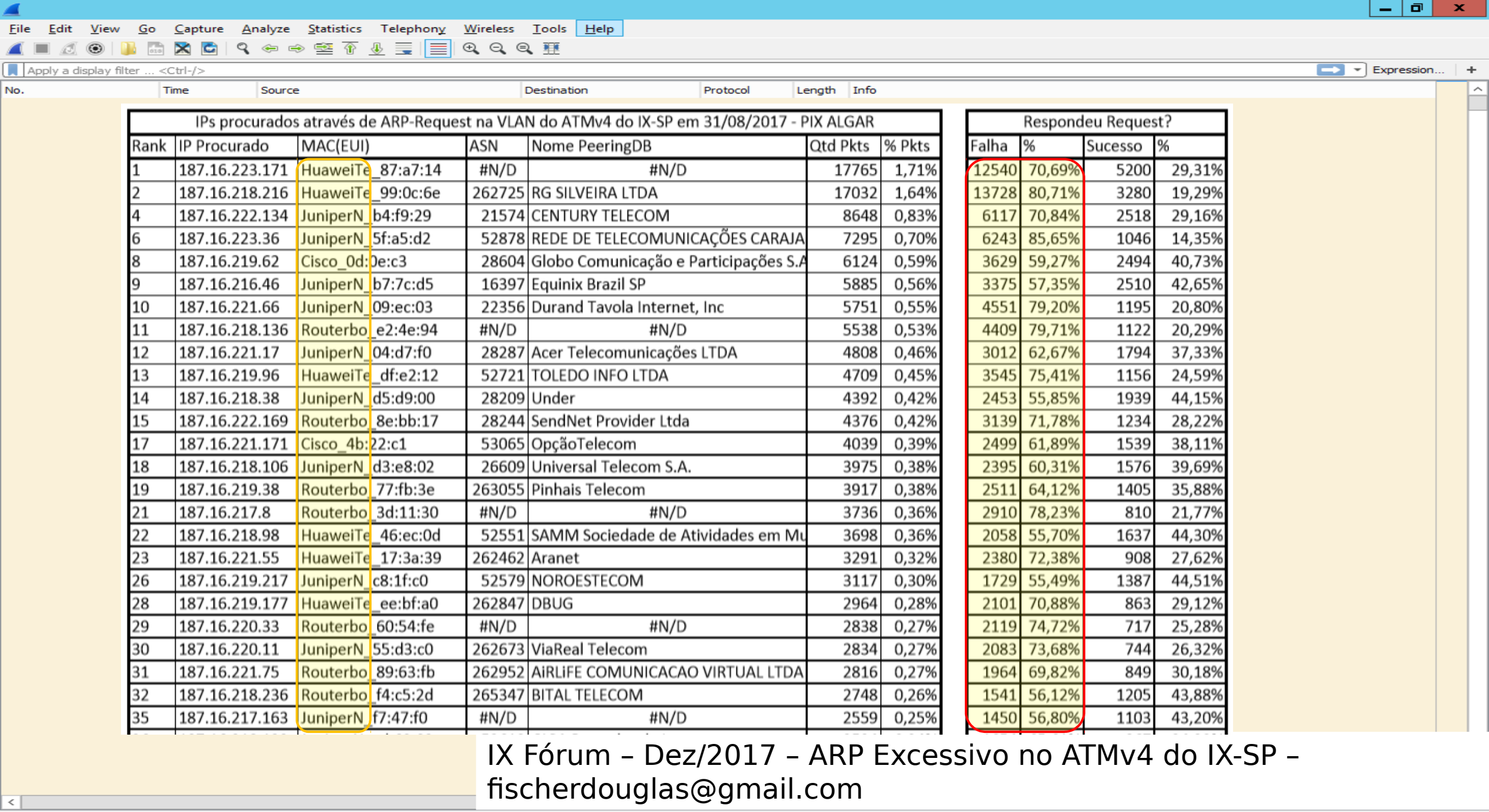
	MAC(EUI)	Qtd Partic.	% Partic.
1	Routerbo	616	48,50%
2	JuniperN	245	19,29%
3	IntelCor	76	5,98%
4	Cisco	71	5,59%
5	Ubiquiti	44	3,46%
6	HuaweiTe	35	2,76%
7	Dell	32	2,52%
8	Serveru	28	2,20%
9	Broadcom	15	1,18%
10	BrocadeC	12	0,94%



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 – fischerdouglas@gmail.com



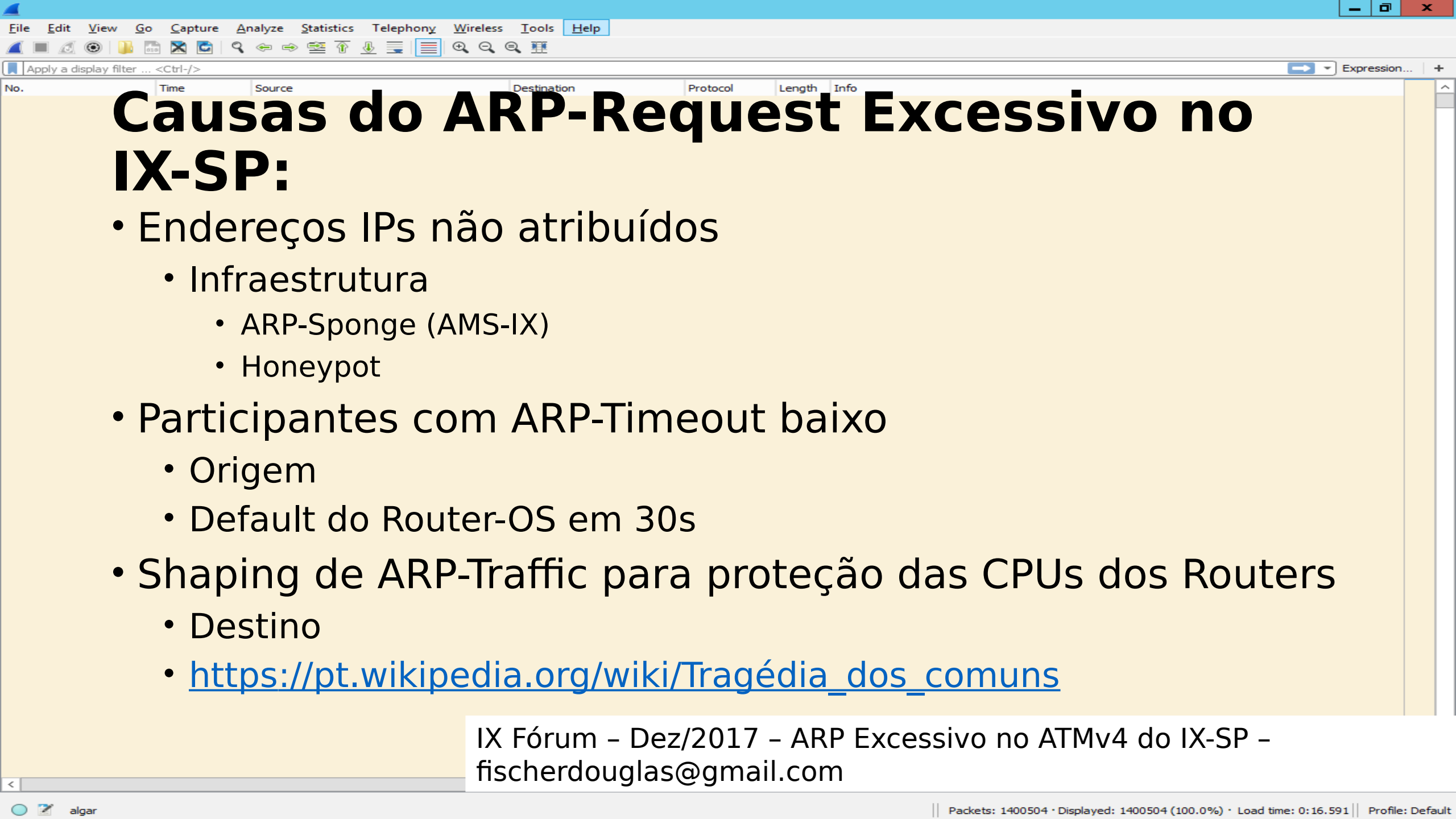
IPs procurados através de ARP-Request na VLAN do ATMv4 do IX-SP em 31/08/2017 - PIX ALGAR							Respondeu Request?			
Rank	IP Procurado	MAC(EUI)	ASN	Nome PeeringDB	Qtd Pkts	% Pkts	Falha	%	Sucesso	%
1	187.16.223.171	HuaweiTe_87:a7:14	#N/D	#N/D	17765	1,71%	12540	70,69%	5200	29,31%
2	187.16.218.216	HuaweiTe_99:0c:6e	262725	RG SILVEIRA LTDA	17032	1,64%	13728	80,71%	3280	19,29%
4	187.16.222.134	JuniperN_b4:f9:29	21574	CENTURY TELECOM	8648	0,83%	6117	70,84%	2518	29,16%
6	187.16.223.36	JuniperN_5f:a5:d2	52878	REDE DE TELECOMUNICAÇÕES CARAJA	7295	0,70%	6243	85,65%	1046	14,35%
8	187.16.219.62	Cisco_0d:0e:c3	28604	Globo Comunicação e Participações S.A	6124	0,59%	3629	59,27%	2494	40,73%
9	187.16.216.46	JuniperN_b7:7c:d5	16397	Equinix Brazil SP	5885	0,56%	3375	57,35%	2510	42,65%
10	187.16.221.66	JuniperN_09:ec:03	22356	Durand Tavola Internet, Inc	5751	0,55%	4551	79,20%	1195	20,80%
11	187.16.218.136	Routerbo_e2:4e:94	#N/D	#N/D	5538	0,53%	4409	79,71%	1122	20,29%
12	187.16.221.17	JuniperN_04:d7:f0	28287	Acer Telecomunicações LTDA	4808	0,46%	3012	62,67%	1794	37,33%
13	187.16.219.96	HuaweiTe_df:e2:12	52721	TOLEDO INFO LTDA	4709	0,45%	3545	75,41%	1156	24,59%
14	187.16.218.38	JuniperN_d5:d9:00	28209	Under	4392	0,42%	2453	55,85%	1939	44,15%
15	187.16.222.169	Routerbo_8e:bb:17	28244	SendNet Provider Ltda	4376	0,42%	3139	71,78%	1234	28,22%
17	187.16.221.171	Cisco_4b:22:c1	53065	OpçãoTelecom	4039	0,39%	2499	61,89%	1539	38,11%
18	187.16.218.106	JuniperN_d3:e8:02	26609	Universal Telecom S.A.	3975	0,38%	2395	60,31%	1576	39,69%
19	187.16.219.38	Routerbo_77:fb:3e	263055	Pinhais Telecom	3917	0,38%	2511	64,12%	1405	35,88%
21	187.16.217.8	Routerbo_3d:11:30	#N/D	#N/D	3736	0,36%	2910	78,23%	810	21,77%
22	187.16.218.98	HuaweiTe_46:ec:0d	52551	SAMM Sociedade de Atividades em Mu	3698	0,36%	2058	55,70%	1637	44,30%
23	187.16.221.55	HuaweiTe_17:3a:39	262462	Aranet	3291	0,32%	2380	72,38%	908	27,62%
26	187.16.219.217	JuniperN_c8:1f:c0	52579	NOROESTECOM	3117	0,30%	1729	55,49%	1387	44,51%
28	187.16.219.177	HuaweiTe_ee:bf:a0	262847	DBUG	2964	0,28%	2101	70,88%	863	29,12%
29	187.16.220.33	Routerbo_60:54:fe	#N/D	#N/D	2838	0,27%	2119	74,72%	717	25,28%
30	187.16.220.11	JuniperN_55:d3:c0	262673	ViaReal Telecom	2834	0,27%	2083	73,68%	744	26,32%
31	187.16.221.75	Routerbo_89:63:fb	262952	AiRLiFE COMUNICACAO VIRTUAL LTDA	2816	0,27%	1964	69,82%	849	30,18%
32	187.16.218.236	Routerbo_f4:c5:2d	265347	BITAL TELECOM	2748	0,26%	1541	56,12%	1205	43,88%
35	187.16.217.163	JuniperN_f7:47:f0	#N/D	#N/D	2559	0,25%	1450	56,80%	1103	43,20%

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



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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info

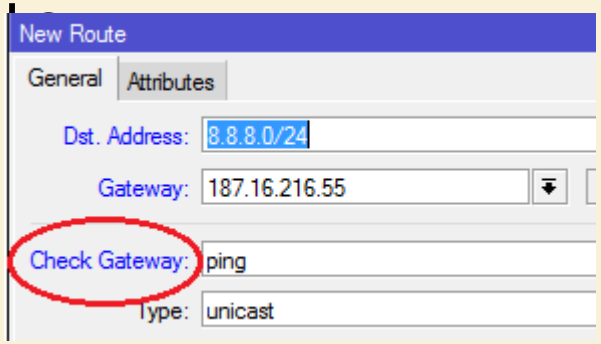
PeeringDB

IX.br (PTT.br) São Paulo

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

2046 hosts que o atual /21 permi

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

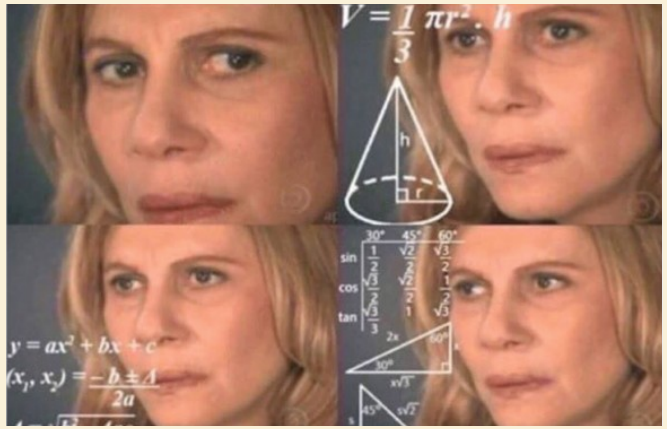


Todo mundo fala com todo mundo

Sem Shaping de ARP

algar

Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 Profile: Default



Extrapolação ARP-Requests IX-SP

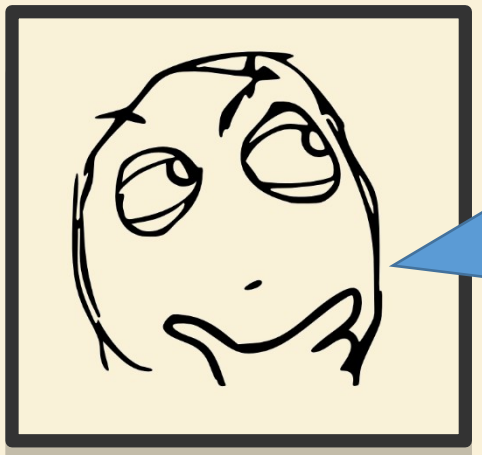
Por Participante

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



“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

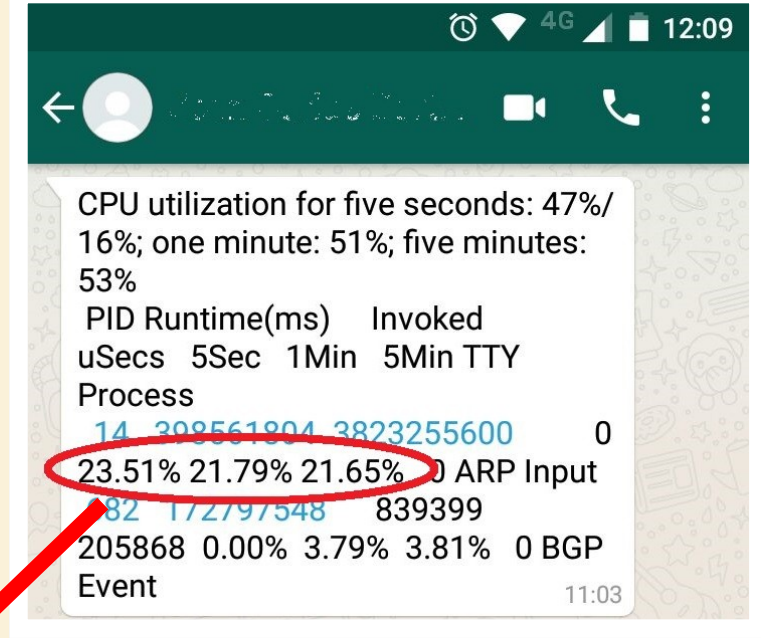
Coleta de 31/08/2017

- 1.287 PPS de ARP-Request
- 1270 Hosts

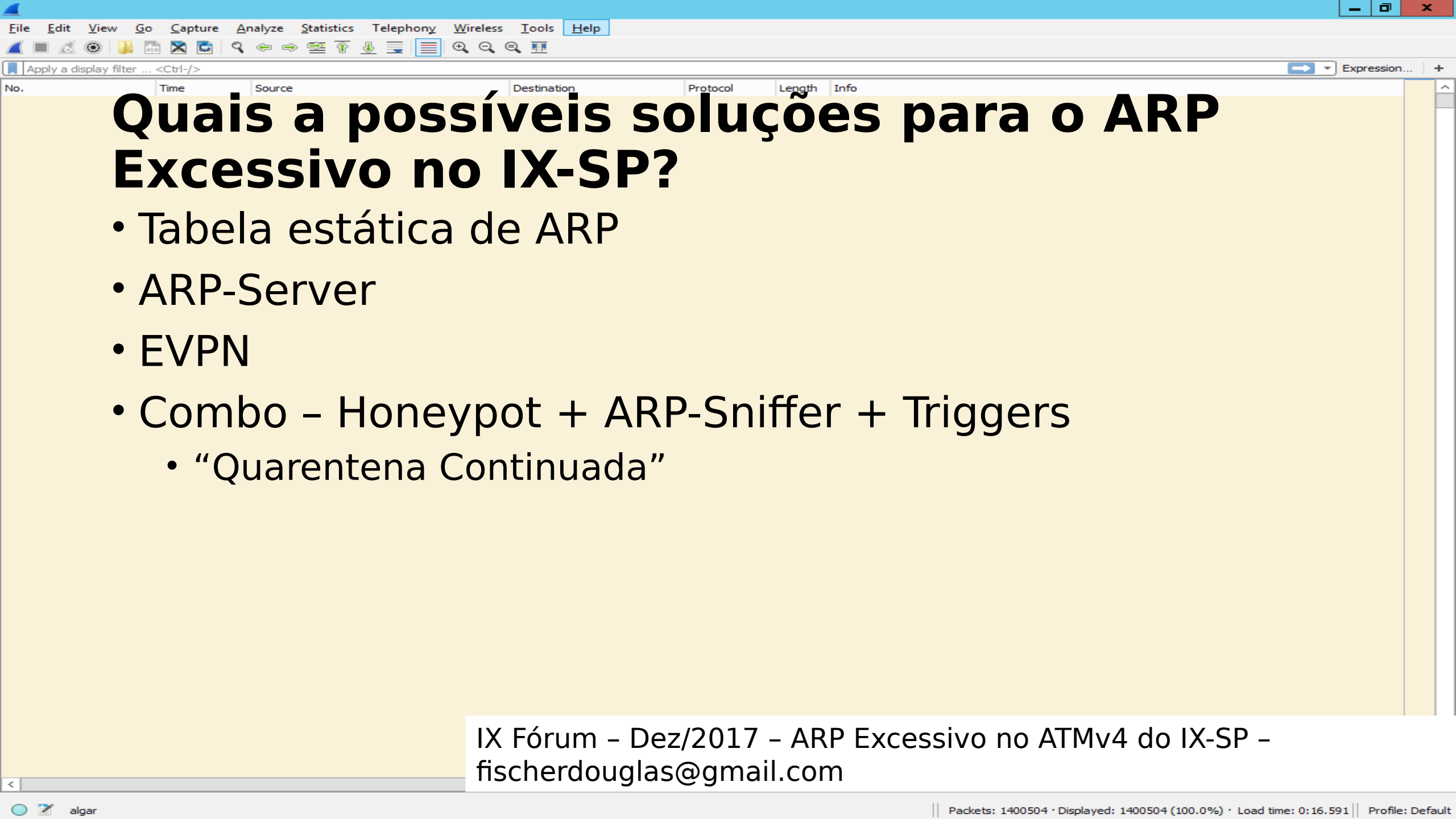
Cenário Hipotético ideal (4h)

- 291 PPS de ARP-Request
- 2046 Hosts

Redução de 4,42 X



4,89 %

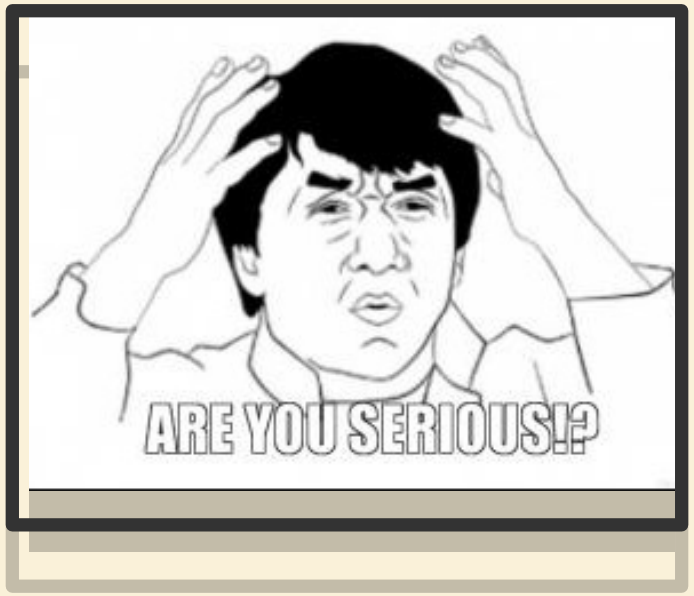


Quais a possíveis soluções para o ARP Excessivo no IX-SP?

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

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)



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

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

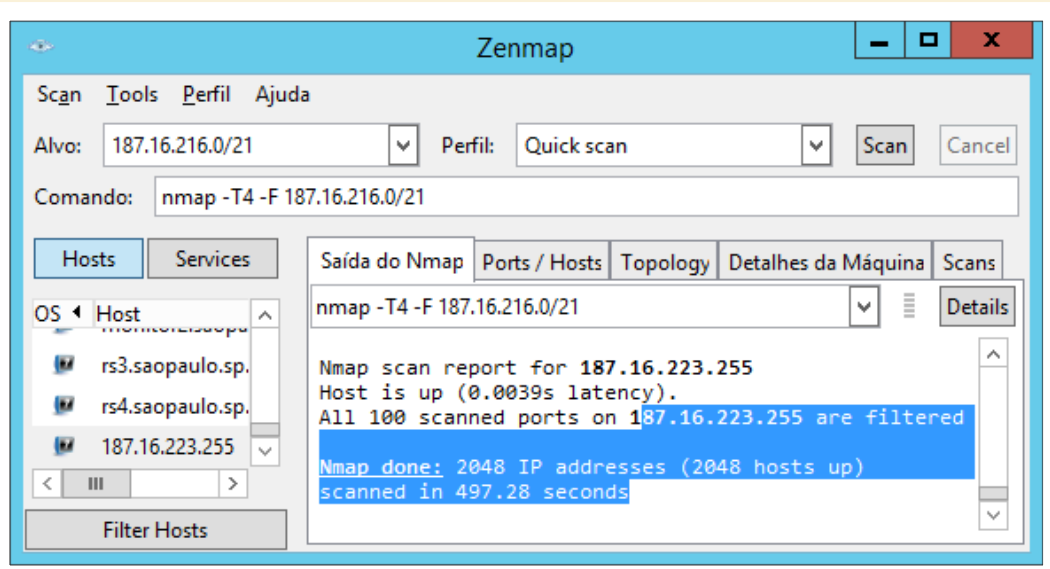
Soluções ARP Excessivo IX – Combo Mágico

- 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

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-Alpha



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No. Time Source Destination Protocol Length Info

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-Alpha

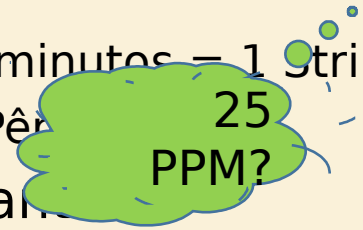
Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 Profile: Default

Combo Mágico – Triggers

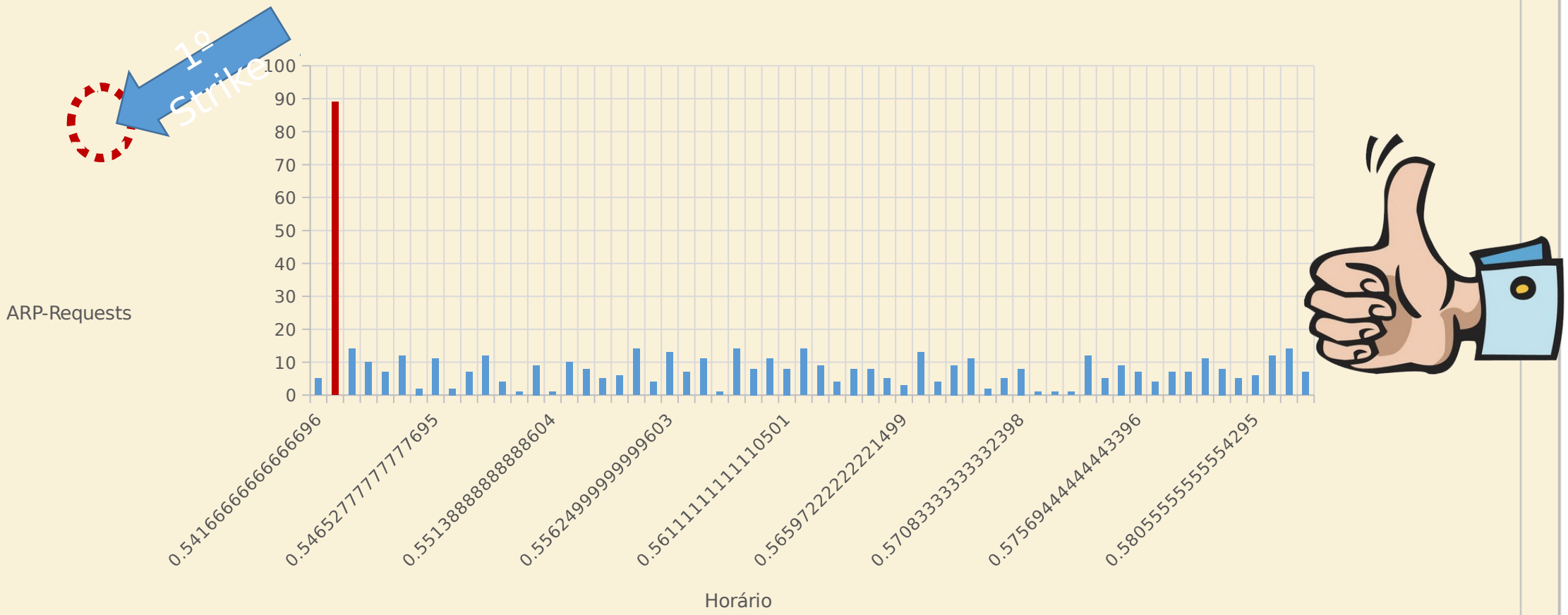
- Tolerâncias
  - Rajadas Verdadeiras
    - Falhas de conectividade do Participante/Transporte
    - Falhas nos Route-Servers
    - Falhas em algum PIX específico ou até generalizada
  - Coincidência temporal de Expiração de ARP-Entries
    - 4 horas depois de um Up/Down de Interface
    - 4 horas depois da convergência de rotas(Checkgateway)
- Métrica de análise de conformidade
  - ARP-Requests emitidos pelo participante
    - 1 ou mais Timeslots excedidos últimos 10 minutos = 1 Stril
    - 3 ou mais Strikes na ultima uma hora = 1 Pên
  - ARP-Requests emitidos contra o participan
    - Indicar Shaping a

ARP-Requests 1 host ARP-Timeout de 4h Contra 2046 hosts(/21)	
Pacotes por Segundo	0,142
Pacotes por Minuto	**8,525**
Pacotes por 5 minutos	42,65
Pacotes por Hora	511,

Apenas Ideias!
E ainda estão em
Release Pré-Alpha



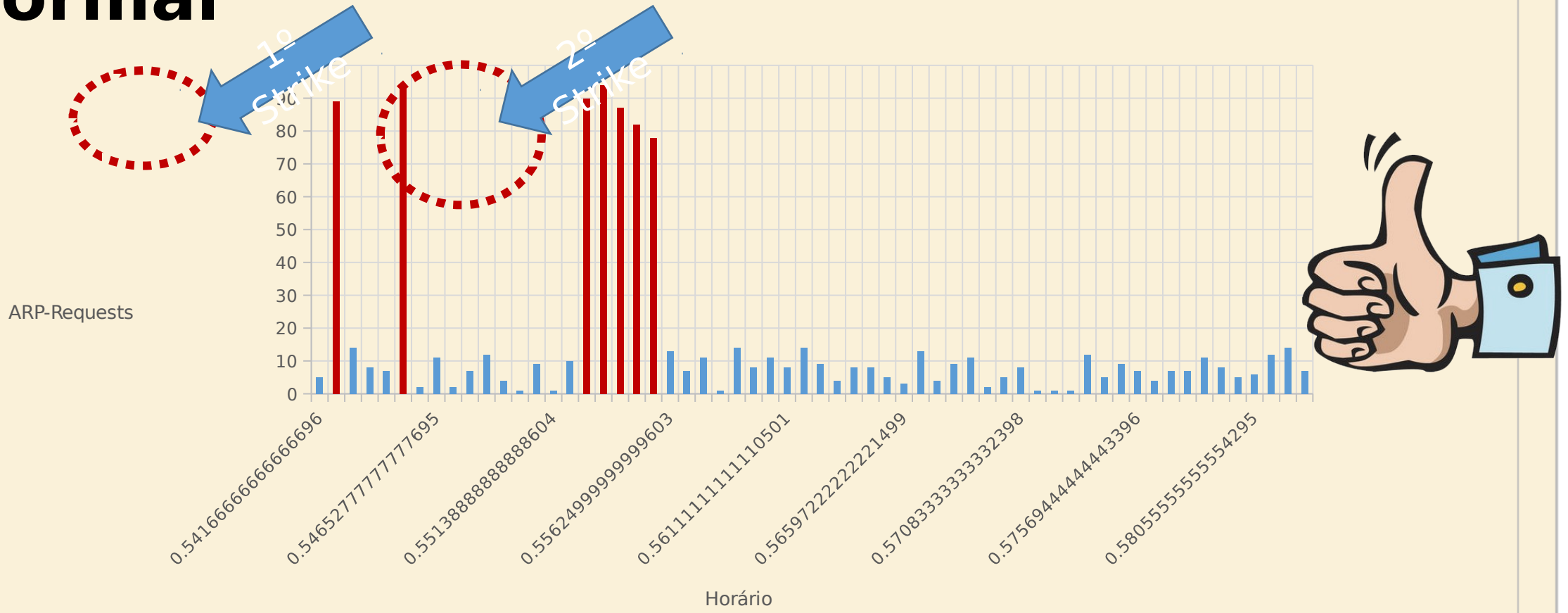
ARP-Requests – Um participante – Ideal



Apenas Ideias!
E ainda estão em Release Pré-Alpha

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

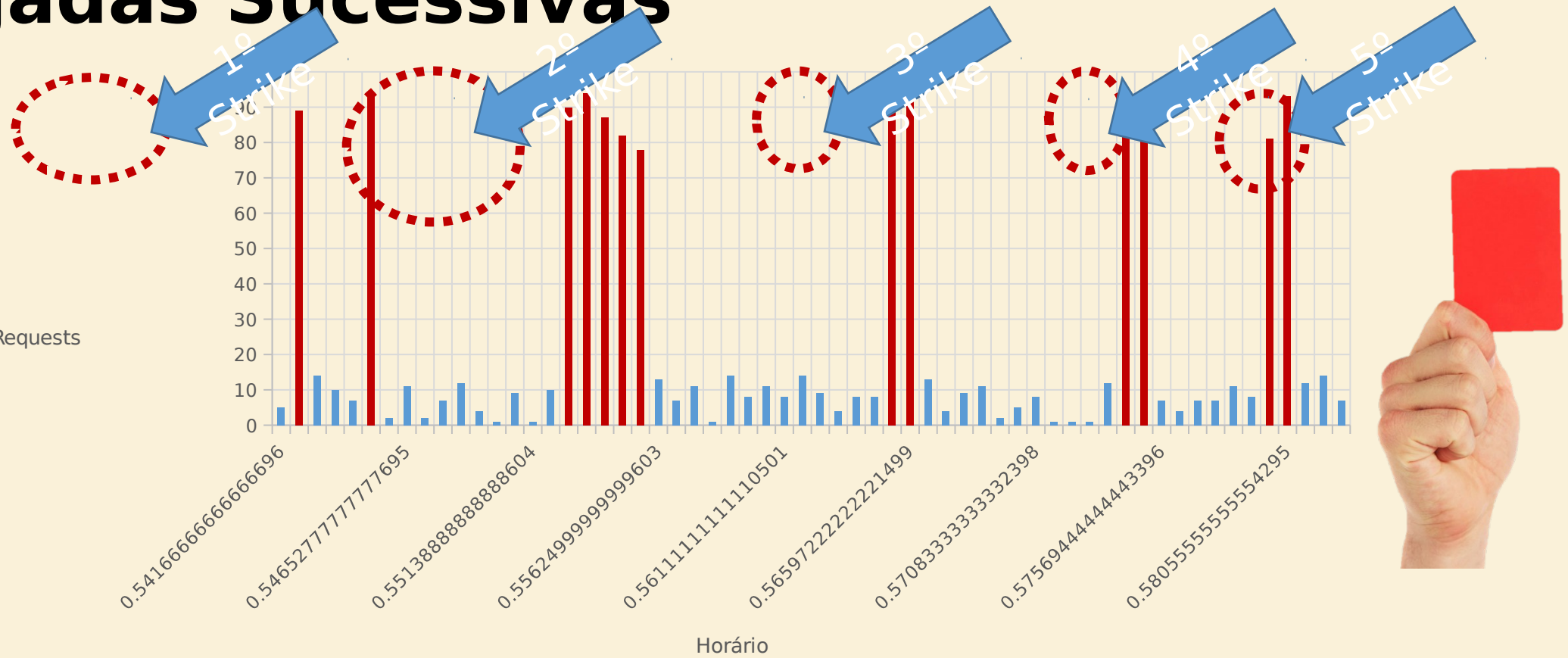
ARP-Requests – Um participante – Normal



Apenas Ideias!
E ainda estão em Release Pré-Alpha

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

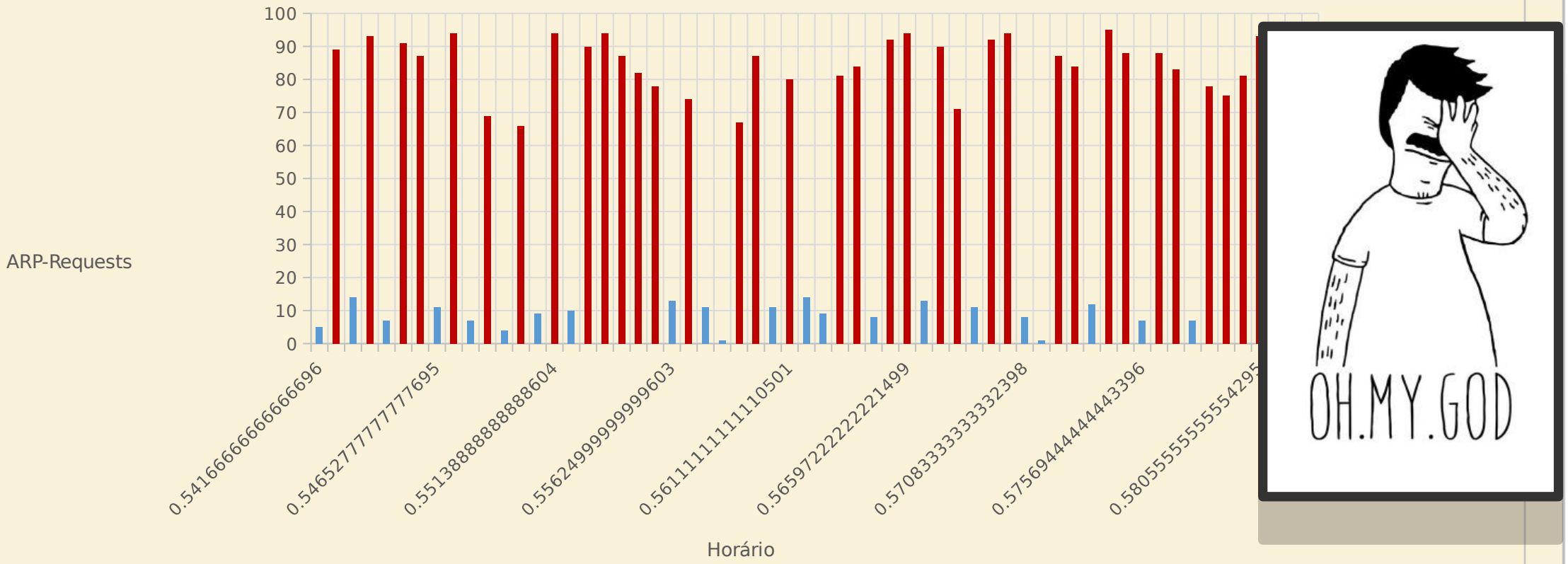
ARP-Requests – Um participante – Rajadas Sucessivas



Apenas Ideias!
E ainda estão em Release Pré-Alpha

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info

Combo Mágico – Ações

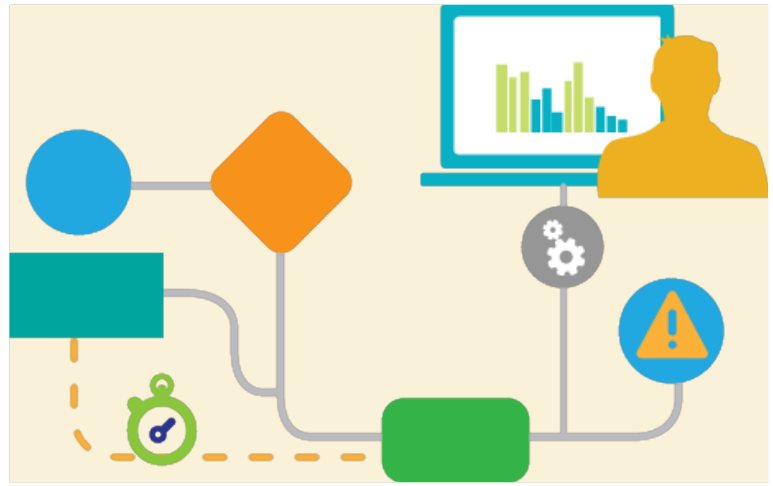
- Notificação automatizada aos responsáveis pelo host que gerou não conformidade
  - Prazo de X horas comerciais(SPO) para correção do problema
- Gratuitous-ARP of Death
  - Host específico emitirá rajadas de ARP-Gratuito com um Mac-Address falso
- API (ou Ansible) – Route-Servers
  - Clear na sessão 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-Alpha

Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 Profile: Default

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

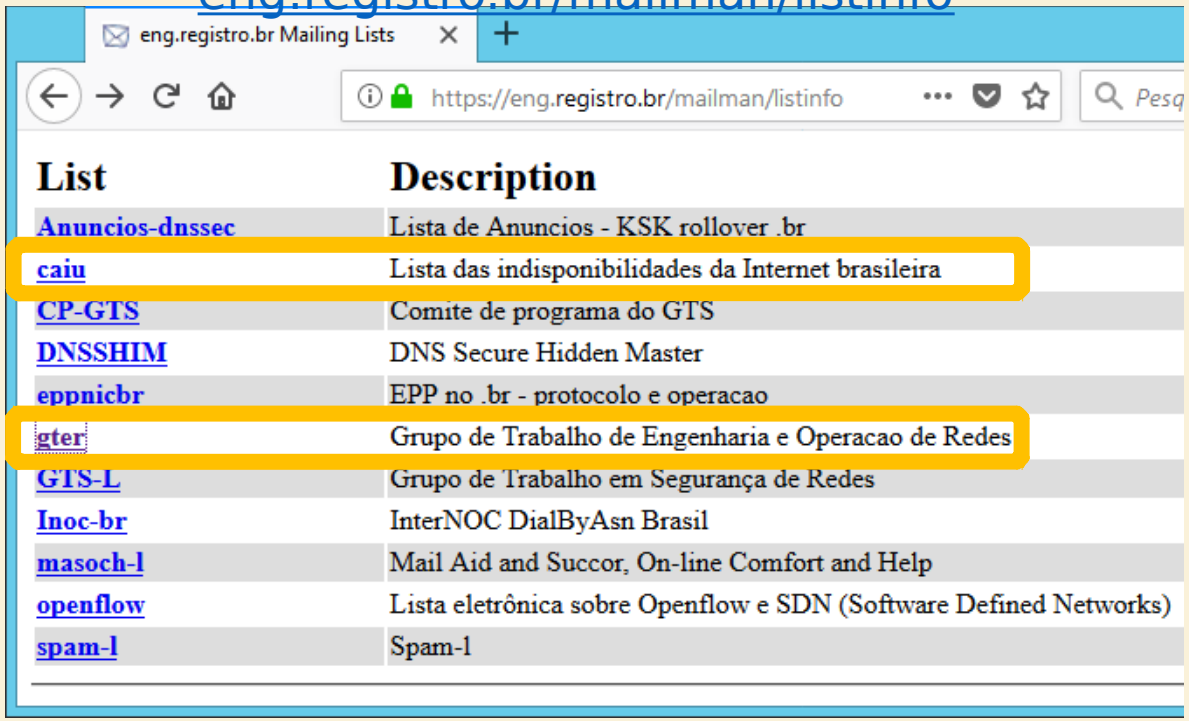


Apenas Ideias!
E ainda estão em Release Pré-Alpha

Locais de troca de informação sobre IX.BR

http://
t.me/ix_br_usuarios

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

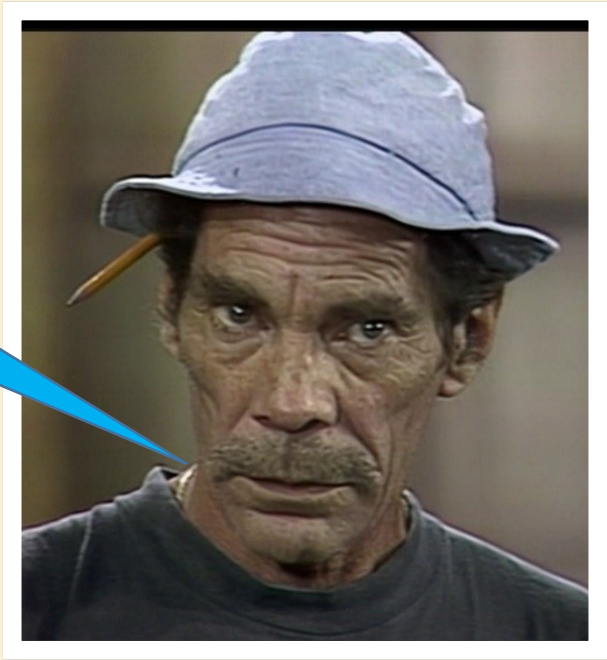


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info

Perguntas?



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

algar

Packets: 1400504 · Displayed: 1400504 (100.0%) · Load time: 0:16.591 Profile: Default