

LACNOG 2018

24 a 28 de Setembro de 2018

Análise de ARP Storm em redes de Internet Exchanges

Desenvolvimento de um mecanismo automatizado

Autor: Douglas Fernando Fischer – fischerdouglas@gmail.com

Douglas Fernando Fischer

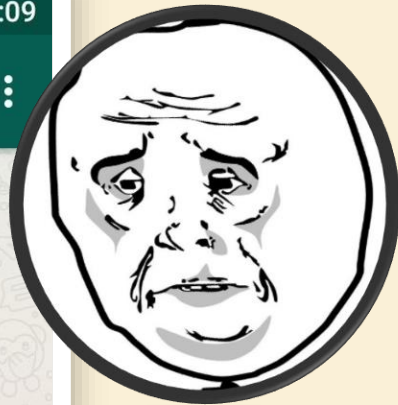
- Engenheiro de Controle e Automação
- Atua na área de redes de telecomunicações desde 1999
- Trabalhou como engenheiro de pré-vendas e implantação em integradores de tecnologia
- Consultor na área de redes e servidores no segmento corporativo e provedores de Internet
- Unioeste – Responsável pela área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

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

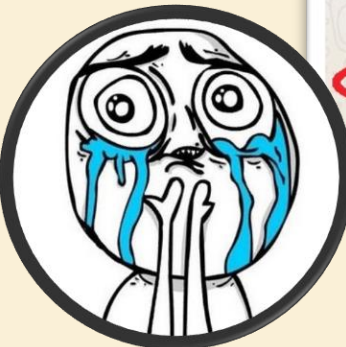
Como eu comecei a me interessar pela questão do ARP em ambiente de IX?

Software-based vs Hardware-based Routers

```
SPO- XXXXXXXX 2#sh proc cpu sor | e
0.00
PID Runtime(ms)  Invoked
uSecs 5Sec 1Min 5Min TTY
Process
14 193878384 1338451946
14 8.24% 8.61% 8.27% ARP
Input
11:54
```

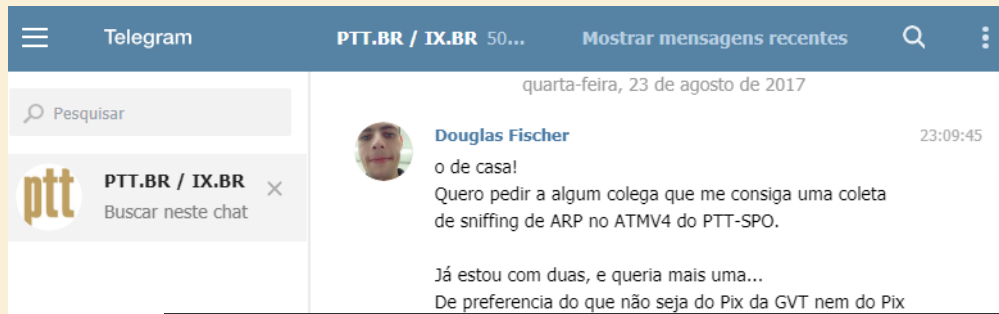


```
CPU utilization for five seconds: 47%/
16%; one minute: 51%; five minutes:
53%
PID Runtime(ms)  Invoked
uSecs 5Sec 1Min 5Min TTY
Process
14 209561804 3823255600 0
23.51% 21.79% 21.65% ARP Input
682 172797548 839399
205868 0.00% 3.79% 3.81% 0 BGP
ent
11:03
```



LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

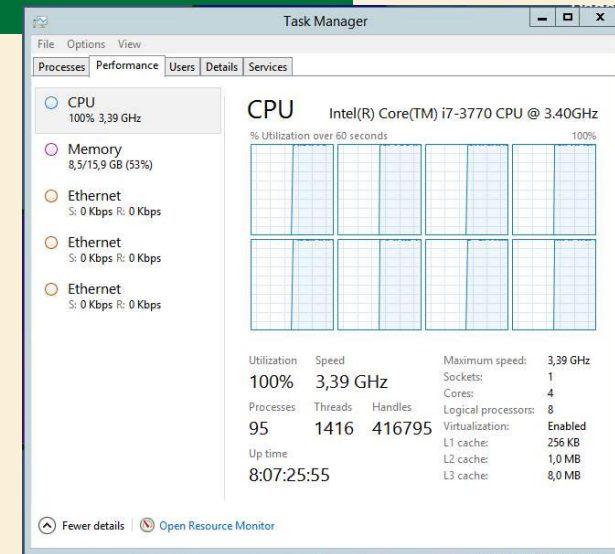
E agora? O que eu posso fazer?



Wireshark capture of network traffic. The main pane shows a list of captured packets, all of which are ARP requests. The details pane shows the structure of an ARP request frame.

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)



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



Porque tá rolando tanto ARP nessa rede?

Análise dos pacotes de Brodcasts transmitidos no IX-SP
Capturas realizadas em múltiplos 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	5,87%

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 - Procurados			
	MAC(EUI)	Qtd Pkts	% Pkts
1	Routerbo	303878	29,17%
2	#N/D	302170	29,01%
3	JuniperN	179692	17,25%
4	HuaweiTe	72954	7,00%
5	Cisco	47541	4,56%
6	IntelCor	38788	3,72%
7	Serveru	20092	1,93%

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%

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%

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



IX (PTT) Fórum 11: ARP excessivo no barramento do ATMv4 do IX-SP - Análise de causas, problemas e...
NICbrvideos • 344 visualizações • 8 meses atrás
A 11ª edição do IX (PTT) Fórum ocorreu de 04 a 05 de dezembro de 2017, em São Paulo, durante a VII Semana da Infraestrutura ...

[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://youtu.be/TgFIRXCxRXO>

<http://forum.ix.br/files/apresentacao/arquivo/159/05%2012%20%2016%2050%20%20Douglas.pdf>

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

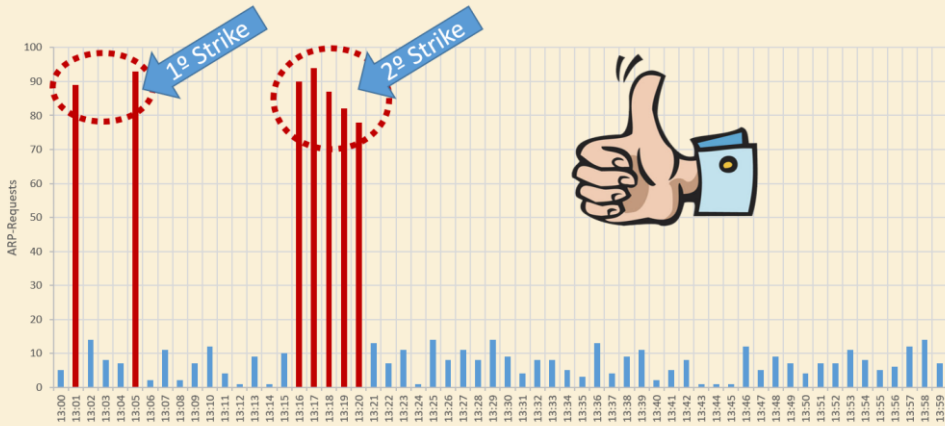
LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

Causas do ARP-Request Excessivo no IX-SP:

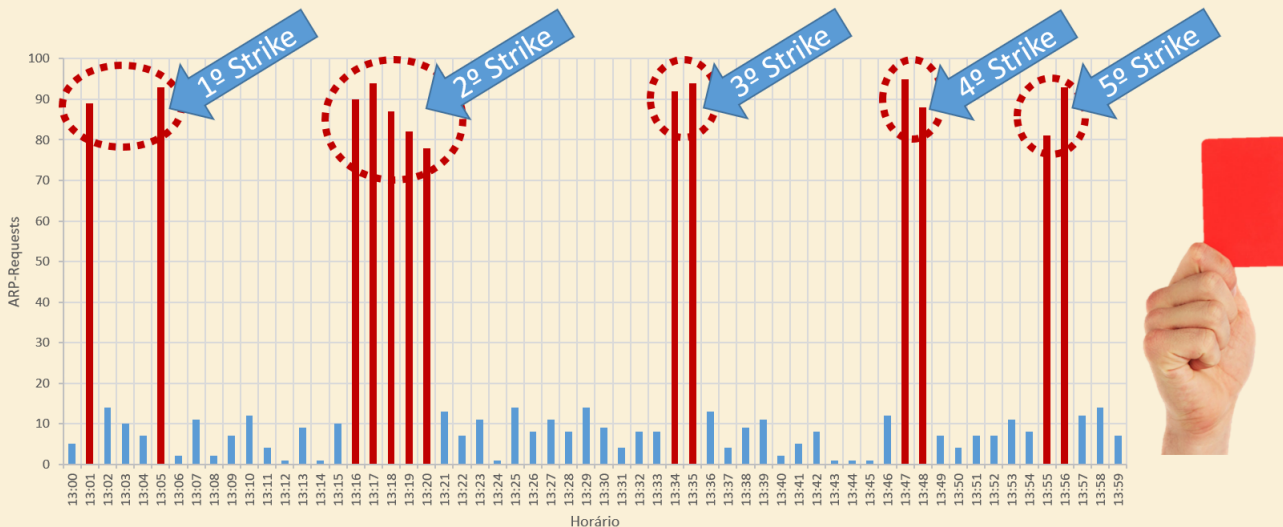
- Endereços IPs não atribuídos
 - Infraestrutura
- Participantes com ARP-Timeout baixo
 - Origem
 - Default do Router-OS em 30s
- Shaping de ARP-Traffic para proteção das CPUs dos Routers
 - Destino
 - [https://pt.wikipedia.org/wiki/Tragédia dos comuns](https://pt.wikipedia.org/wiki/Tragédia_dos_comuns)

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

ARP-Requests – Um participante – Normal



ARP-Requests – Um participante – Rajadas Sucessivas



Sugestões Feitas para conter o ARP Excessivo



- Triggers - Métrica de análise de conformidade
 - ARP-Requests emitidos pelo participante
 - 25 PPM
 - 1 ou mais Timeslots excedidos nos últimos 10 minutos = 1 Strike
 - 3 ou mais Strikes na ultima uma hora = 1 Pênalti

ARP-Bait (Honeypot)

- Host simples com todos os IPsv4 não atribuídos como secundário
 - Atribuição desse IPs de forma automatizada a partir da base de gerência do IX
 - Só responde a ARP e a ICMP

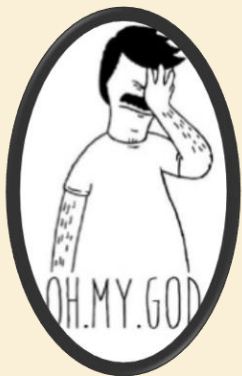
Hall of Shame do Broadcast no ATM(MLPA)

Lista pública de quem seriam os maiores causadores de ARP-Excessivo

- Por origem
- Por destino

Outros tipos de Broadcasts nas Vlans de ATM

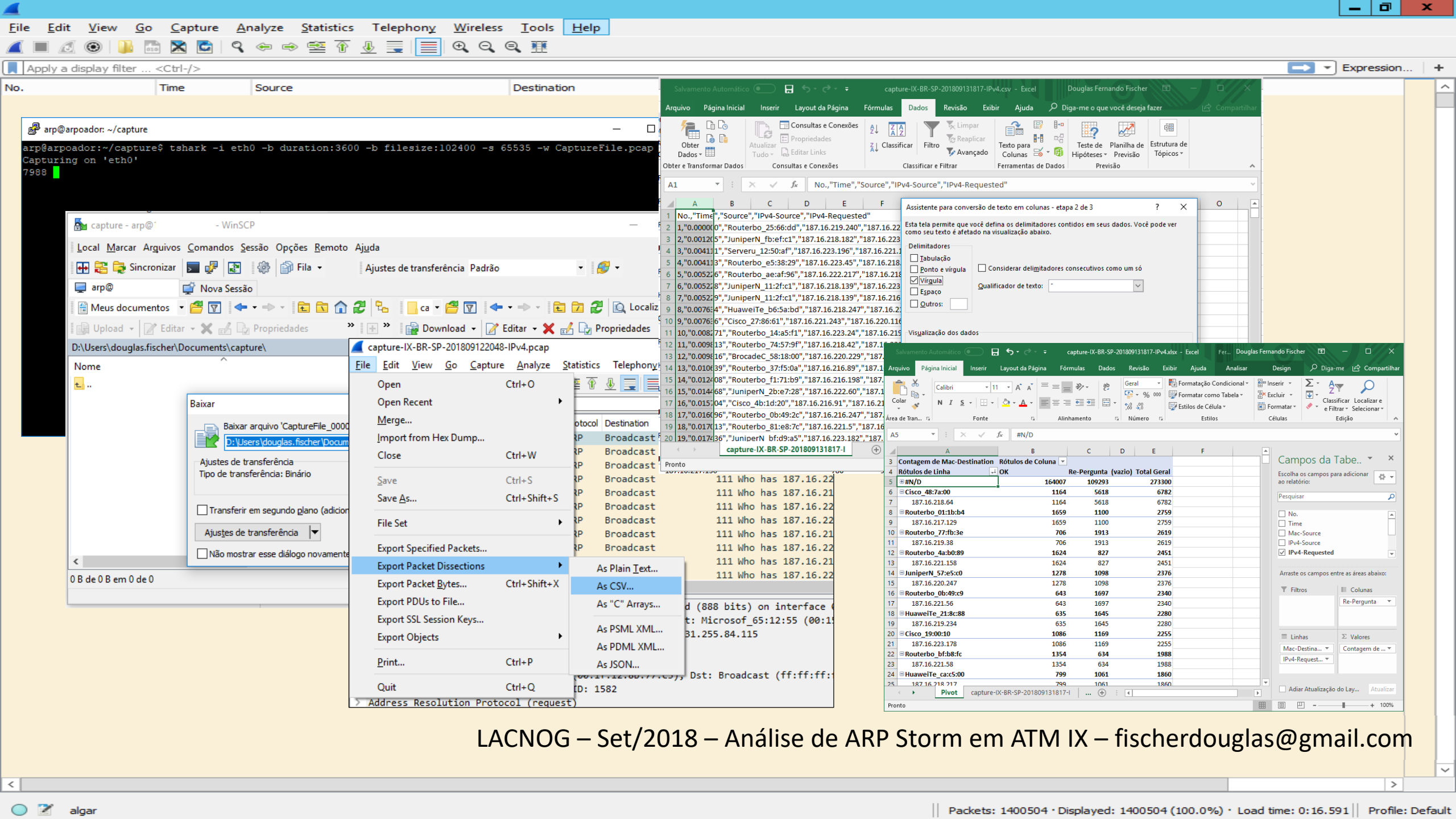
- ARP Requests fora da faixa de rede
- OSPF/RIP
- DHCP Requests
- PPPoE PADI



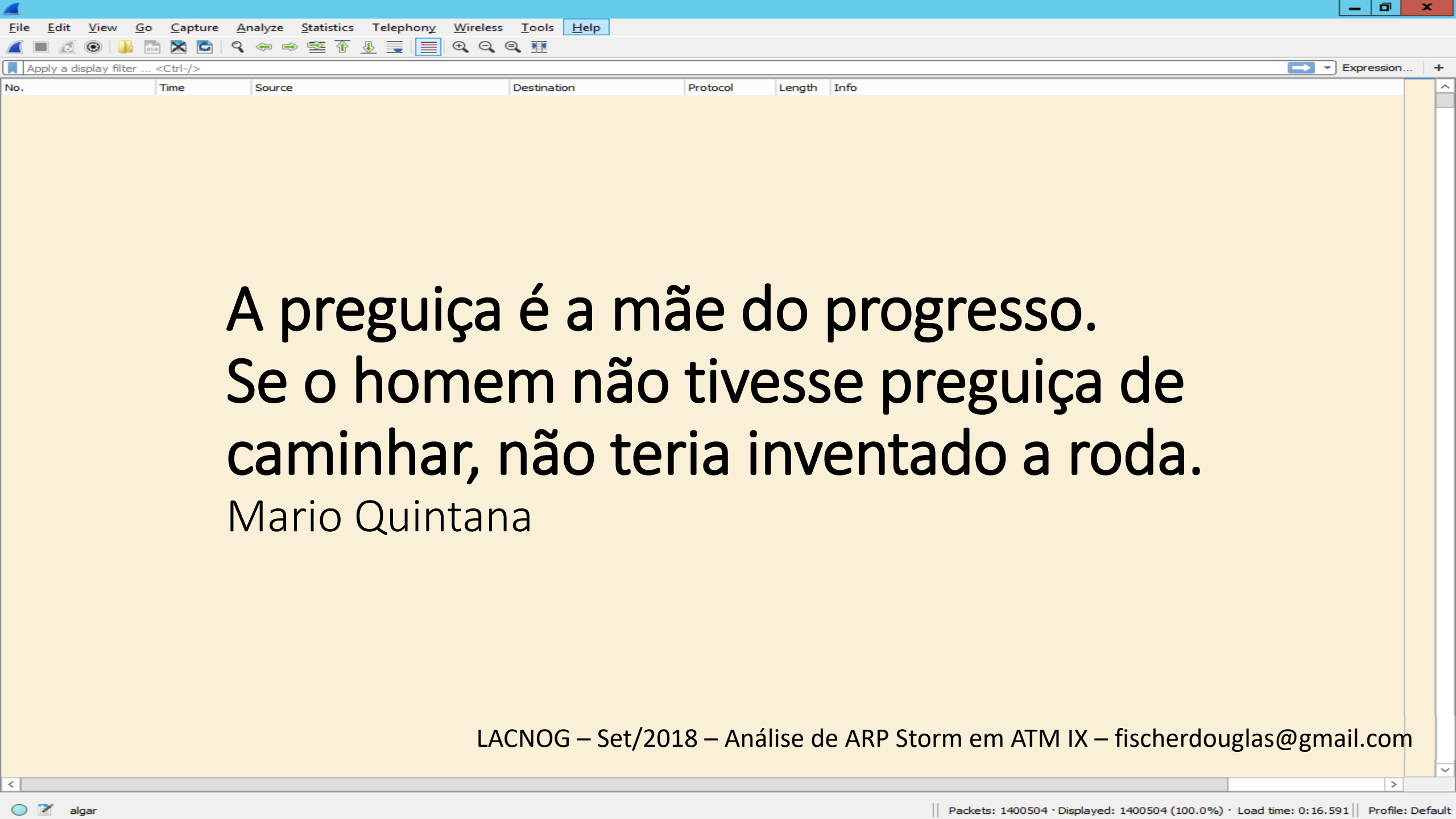
Oi Douglas...
Ajustei o ARP-Timeout da minha CCR.
Pode ver se ainda estou nos TOP 20?

2-3x por dia

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com



LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglass@gmail.com



A preguiça é a mãe do progresso.
Se o homem não tivesse preguiça de
caminhar, não teria inventado a roda.
Mario Quintana


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

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

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>



LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

algar

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

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>



- Aquisição de amostras dos Broadcasts
 - Só precisa “escutar” os pacotes Broadcast
 - Estender as Vlans do ATM Diretamente até a Virtual Machine do ARPOADOR
 - Estender as Vlans do ATM através Algum protocolo L2overL3 (PW, VXlan, EoIP) até a VM do ARPOADOR
 - Usar TaZmen Sniffer Protocol (TZSP) e enviar para encapsulado para Virtual Machine do ARPOADOR
- Capturas cíclicas de 1 em 1 minuto
 - Utilizando tshark para maior granularidade na filtragem e também suportar TZSP
- Processamento
 - Usando dissectors
 - Split dos PCAPs em IPv4, IPv6, e não conformidades
 - Contabilização por Origem e Destino de IPv4 e IPv6
 - Contabilização por origem de não conformidades
- Saída
 - Exportado para arquivos CSV

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>

Resultados IPv4

No.	Time	Source	Destination	Protocol	Length	Info
1						IPv4-Requested, Quantity
2						187.16.217.4, 1212
3						187.16.218.64, 966
4						187.16.216.139, 822
5						187.16.221.189, 683
6						187.16.218.174, 601
7						187.16.222.65, 537
8						187.16.218.229, 526
9						187.16.219.49, 443
10						187.16.218.66, 410
11						187.16.221.118, 396
12						187.16.220.155, 391
13						187.16.219.38, 359
14						187.16.218.49, 345
15						187.16.223.178, 293
16						187.16.223.236, 270
17						187.16.222.134, 266
18						187.16.219.159, 265
19						187.16.216.116, 255
20						187.16.219.75, 238
21						187.16.218.97, 237
22						187.16.220.111, 235
23						187.16.221.33, 232
24						187.16.222.241, 226
25						187.16.219.11, 226

No.	Time	Source	Destination	Protocol	Length	Info
1						Mac-Source, Quantity, IPv4-Source, MacEUI-Source
2						60:9c:9f:59:d6:00, 1288, 187.16.221.197, BrocadeC_59:d6:00
3						84:44:64:35:ca:28, 1061, 187.16.220.23, Serveru_35:ca:28
4						d4:ca:6d:77:c5:20, 948, 187.16.217.231, Routerbo_77:c5:20
5						90:e2:ba:86:cd:a4, 833, 187.16.220.126, IntelCor_86:cd:a4
6						00:15:17:20:c6:ed, 750, 187.16.216.167, IntelCor_20:c6:ed
7						b0:a8:6e:30:47:cb, 716, 187.16.218.82, JuniperN_30:47:cb
8						84:c1:c1:2b:e7:28, 667, 187.16.222.60, JuniperN_2b:e7:28
9						30:b6:4f:0a:52:00, 659, 187.16.222.61, JuniperN_0a:52:00
10						00:24:38:ab:47:06, 585, 187.16.218.137, BrocadeC_ab:47:06
11						f4:e9:d4:a2:3f:52, 562, 187.16.218.112, Qlogic_a2:3f:52
12						88:e0:f3:7e:ce:03, 556, 187.16.223.133, JuniperN_7e:ce:03
13						64:d1:54:38:39:53, 551, 187.16.220.236, Routerbo_38:39:53
14						28:8a:1c:52:69:c0, 539, 187.16.220.181, JuniperN_52:69:c0
15						00:1b:21:81:ca:d6, 486, 187.16.221.203, IntelCor_81:ca:d6
16						ec:38:73:51:b5:c2, 484, 187.16.220.8, ec:38:73:51:b5:c2
17						24:6e:96:7b:a2:c2, 484, 187.16.216.175, Dell_7b:a2:c2
18						60:73:5c:48:30:81, 471, 187.16.216.253, Cisco_48:30:81
19						4c:5e:0c:02:98:46, 469, 187.16.218.105, Routerbo_02:98:46
20						30:f7:0d:b9:e7:01, 412, 187.16.223.253, Cisco_b9:e7:01
21						84:44:64:4c:74:ac, 397, 187.16.216.218, Serveru_4c:74:ac
22						4c:5e:0c:6a:47:5e, 388, 187.16.219.50, Routerbo_6a:47:5e
23						24:6e:96:4c:d6:4a, 387, 187.16.222.244, Dell_4c:d6:4a
24						60:9c:9f:5c:74:41, 378, 187.16.216.48, BrocadeC_5c:74:41
25						a4:ba:db:08:9f:9b, 365, 187.16.220.84, Dell_08:9f:9b

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>

Resultados IPv6

IPV6-Requested, Quantity
2001:12f8::218:227, 1525
2001:12f8::222:39, 1428
2001:12f8::223:89, 1418
2001:12f8::223:128, 1399
2001:12f8::222:78, 1353
2001:12f8::219:42, 1321
2001:12f8::223:254, 1215
2001:12f8::223:50, 1104
2001:12f8::223:211, 841
2001:12f8::222:216, 478
2001:12f8::217:59, 473
2001:12f8::221:224, 421
2001:12f8::221:223, 420
2001:12f8::217:143, 327
2001:12f8::218:168, 308
2001:12f8::223:180, 297
2001:12f8::221:190, 290
2001:12f8::219:132, 288
2001:12f8::11, 285
2001:12f8::220:232, 284
2001:12f8::222:192, 268
2001:12f8::217:42, 263
2001:12f8::221:158, 259
2001:12f8::222:25, 254

Mac-Source, Quantity, IPv6-Source, MacEUI-Source
74:8e:f8:a5:82:81, 4275, 2001:12f8::218:55, BrocadeC_a5:82:81
90:b1:1c:1d:d7:19, 443, 2001:12f8::223:254, Dell_ld:d7:19
14:18:77:4b:78:ce, 403, 2001:12f8::253, Dell_4b:78:ce
5c:e0:f6:00:00:21, 382, 2001:12f8::254, NicBr-Nu_00:00:21
14:18:77:4b:08:4d, 342, 2001:12f8::223:253, Dell_4b:08:4d
d0:43:1e:45:e1:fa, 157, 2001:12f8::252, Dell_45:e1:fa
5c:45:27:7b:5b:03, 140, 2001:12f8::219:111, JuniperN_7b:5b:03
5c:5e:ab:b9:70:f9, 125, 2001:12f8::218:79, JuniperN_b9:70:f9
d8:b1:22:c7:a6:26, 118, 2001:12f8::219:83, JuniperN_c7:a6:26
f4:b5:2f:fc:1f:c3, 117, 2001:12f8::218:58, JuniperN_fc:1f:c3
3c:94:d5:11:3f:cd, 110, 2001:12f8::218:144, JuniperN_11:3f:cd
3c:94:d5:11:2f:c1, 95, 2001:12f8::218:139, JuniperN_11:2f:c1
b0:a8:6e:2f:ff:c2, 92, 2001:12f8::220:240, JuniperN_2f:ff:c2
b0:a8:6e:30:47:cb, 89, 2001:12f8::218:82, JuniperN_30:47:cb
00:1f:12:8b:77:c3, 79, 2001:12f8::55, JuniperN_8b:77:c3
78:19:f7:35:f8:55, 72, 2001:12f8::217:20, JuniperN_35:f8:55
f0:1c:2d:8e:4e:c6, 59, 2001:12f8::220:213, JuniperN_8e:4e:c6
00:c1:64:27:86:61, 53, 2001:12f8::221:243, Cisco_27:86:61
00:1b:21:ae:a8:9d, 53, 2001:12f8::217:75, IntelCor_ae:a8:9d
88:e0:f3:7e:ce:03, 51, 2001:12f8::223:133, JuniperN_7e:ce:03
30:b6:4f:0a:52:00, 49, 2001:12f8::222:61, JuniperN_0a:52:00
ec:38:73:51:b5:c3, 48, 2001:12f8::220:8, ec:38:73:51:b5:c3
84:44:64:67:e5:55, 48, 2001:12f8::221:218, Serveru_67:e5:55
5c:54:6d:95:c0:53, 43, 2001:12f8::223:185, HuaweiTe_95:c0:53

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>

Resultados Não Conformidades

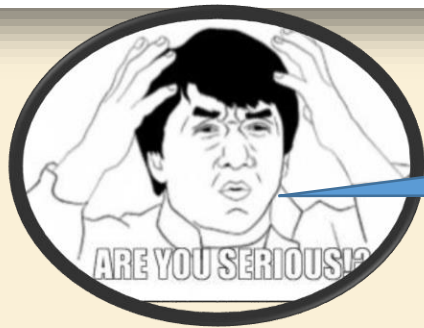
No.	Time	Source	Destination	Protocol	Length	Info
1						Mac-Source, Quantity, Vlan, TypeOfNonConformity, Complement
2						64:d1:54:13:ed:c0, 166, ATMv4, QinQ,
3						e4:8d:8c:1b:b4:a0, 517, ATMv4, Bootp, DHCP
4						e4:8d:8c:1b:b4:a0, 106, ATMv6, Bootp, DHCP
5						4c:5e:0c:25:7e:f4, 9, ATMv4, VendorDiscovery, MNDP
6						64:d1:54:cf:20:d0, 10, ATMv4, VendorDiscovery, MNDP
7						64:d1:54:cf:20:d0, 10, ATMv6, VendorDiscovery, MNDP
8						4c:5e:0c:4a:d7:78, 12, ATMv4, IPv6onATMv4,
9						6c:3b:6b:ea:10:cd, 34, ATMv4, IPv6onATMv4,
10						64:d1:54:cf:20:d0, 10, ATMv6, IPv4onATMv6,
11						c0:67:af:8f:a3:50, 1, ATMv6, IPv4onATMv6,
12						e4:8d:8c:1b:b4:a0, 106, ATMv6, IPv4onATMv6,
13						00:2e:c7:09:2a:53, 120, ATMv4, GratuitousArp, 187.16.222.83
14						00:2e:c7:09:31:99, 238, ATMv4, GratuitousArp, 187.16.216.34
15						04:18:d6:f1:3d:31, 120, ATMv4, GratuitousArp, 187.16.220.78
16						10:51:72:2f:7e:71, 120, ATMv4, GratuitousArp, 187.16.223.58
17						f4:4c:7f:91:b5:a7, 114, ATMv4, GratuitousArp, 187.16.218.2
18						00:0c:42:5f:07:8e, 1, ATMv6, RouterAdvertisement,
19						e4:8d:8c:35:34:51, 1, ATMv6, RouterAdvertisement,
20						00:15:c5:e6:67:34, 1, ATMv4, ARPSourceOutOfRange, 177.10.208.3
21						00:1b:21:81:ca:d6, 2, ATMv4, ARPSourceOutOfRange, 177.130.113.126
22						00:1c:73:0f:78:08, 1, ATMv4, ARPSourceOutOfRange, 131.221.44.1
23						00:1c:73:0f:78:08, 3, ATMv4, ARPSourceOutOfRange, 131.221.44.104
24						00:1a:8c:52:da:98, 14, ATMv4, ARPDstOutOfRange,
25						00:1d:46:c7:0a:d0, 16, ATMv4, ARPDstOutOfRange,

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>

```
## Creating Statistics Files
#List Requested
tshark -r $BaseCaptureFile-IPv4.pcap \
  -o 'gui.column.format:""IPv4-Requested"", ""%Cus:arp.dst.proto_ipv4""'\
  | sort | uniq -c | awk -F ' ' '{print $2"", ""$1}'\
  | sort -t, -k2 -n -r > $StatisticsFile-IPv4-NormalByArpDestination.csv
sed -i 's/ /IPv4-Requested,Quantity\n/' $StatisticsFile-IPv4-NormalByArpDestination.csv
```



Pipe do Pipe do
Pipe do Pipe?
WTF?

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

ARPOADOR

<https://bitbucket.org/fischerdouglas/arpoador/>



Code Quality
=
Beauty of Developer

ARPOADOR - Reengenharia

<https://bitbucket.org/fischerdouglas/arpoador/>



python

+



mongoDB

- PyShark
- PySNMP



“Nada renasce antes que se acabe.

E o sol que desponta tem que anoitecer.”

Vinicius de Moraes

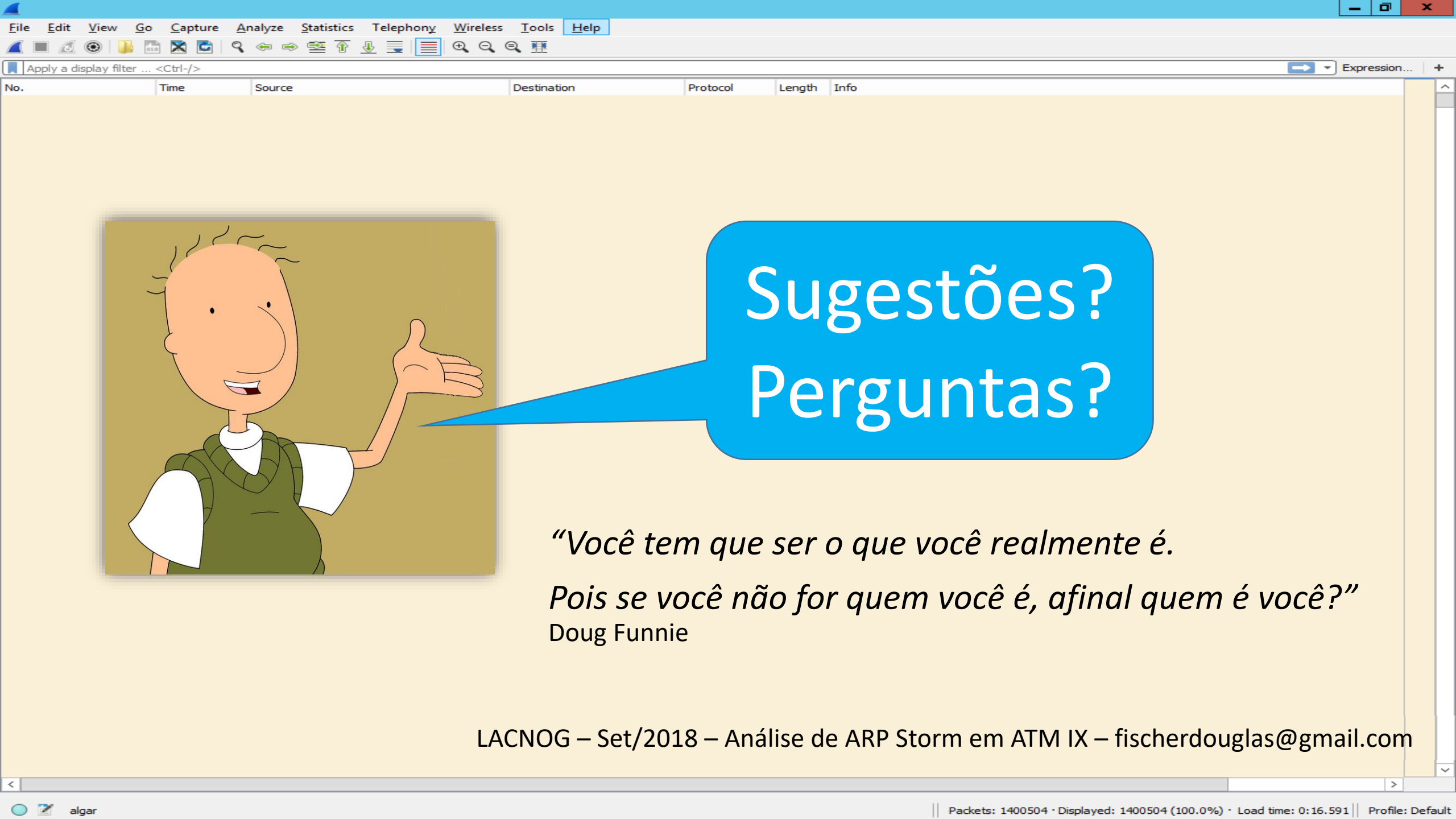
LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com

ARPOADOR - Reengenharia

<https://bitbucket.org/fischerdouglas/arpoador/>

- Aquisição de amostras dos Broadcasts
 - Segue da mesma forma (Direto, TZSP, L2overL3)
 - Receitas de bolo para múltiplos vendedores.
- Captura e Processamento Per-Packet
 - Cada pacote sniffado será classificado e alimentar as tabelas de estatísticas
 - Triggers no Mongo vinculados a Traps de SNMP
 - Ex.: Novos IPs de origem
- Saída
 - HTML, JavaScript e Json
 - Viabilizar Personal Hall Of Shame para cada parti
 - SNMP
 - Subsidiar as Triggers de “Noisy Guys” pelo IX mundo afora

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com



Sugestões?
Perguntas?

“Você tem que ser o que você realmente é.

Pois se você não for quem você é, afinal quem é você?”

Doug Funnie

LACNOG – Set/2018 – Análise de ARP Storm em ATM IX – fischerdouglas@gmail.com