

Security Visualization Tools and IPv6 Addresses

David Barrera P.C. van Oorschot



Canada's Capital University

イロト イポト イヨト イヨト

1/22

Introduction	IPv4 vs IPv6	Problem	Whitespace Filtering	IPv6 Hierarchy	Conclusions

- Introduction
- IPv4 vs. IPv6
- Problem
- Proposal 1: Whitespace filtering
- Proposal 2: IPv6 address hierarchy with treemaps
- Conclusions

- IPv4 address exhaustion predicted to happen in mid-2012 (745 days remaining)¹
- 10% of Class A's remaining
- IPv6 deployment on the global Internet is low (~1%)
- IPv6 deployment inside organizations could be significantly higher

¹http://www.potaroo.net/tools/ipv4/index.html

- IPv6 is already here
- Userspace applications require almost no modifications
- Enabled in new operating systems
- Widely deployed in network tools

- Visualization of IPv6 addresses is difficult
 - Really long numbers (128-bit)
 - Address space is sparsely populated
 - Transition mechanisms interfere with 'real' IPv6 addresses

- Most visualization tools don't support IPv6
 - Assume IPv4
 - Tools are hardcoded to 32-bits
 - Drop/ignore IPv6 packets
 - Crash

Introduction IPv4 vs IPv6 Problem Whitespace Filtering IPv6 Hierarchy Conclusions

Address Representation

- 2001:0DB8:0000:0078:9ABC:0000:0000:0000
- 2001:0DB8:0:0078:9ABC:0:0:0
- 2001:DB8:0:78:9ABC::

Packet Header Changes

- The IPv6 header omits rarely used fields
- IPID, flags, fragment offset, header checksum no longer present
- Flow label is new to the IP header

Introduction

Vhitespace Filtering

IPv6 Hiera

Conclusions

Packet Header Changes

	0-3 4-7 8-15 16-18 19-31						
o	Version	Header Length	Type of Service (ToS)	Total Length			
32	le	dentificat	tion (ID)	Flags	Fragment Offset		
64	Time to Live Protocol Header Checksum						
96			Sour	ce IP Add	fress		
128			Destina	ation IP A	Address		
160							
192							
224							
256	IPv4						
	0-3 4-11 12-15 16-23 24-31						
0	Version Traffic Flow Label						
32	Payload Length			Next Header	Hop Limit		
64							
96	Source IP Address						
128							
160							
192							
224	Destination IP Address						
256							
288	IPv6						

≣ ∽ 8/22

- DHCPv6 and address auto-configuration
- ICMPv6
- Multicast, scope IDs
- New security issues to visualize

ヘロト 人間 とくほ とくほ とう

э

10/22

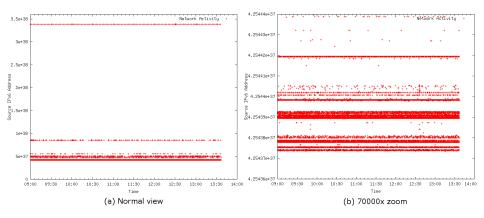
- Capture raw data
- Parse
- Process and reformat
- Display



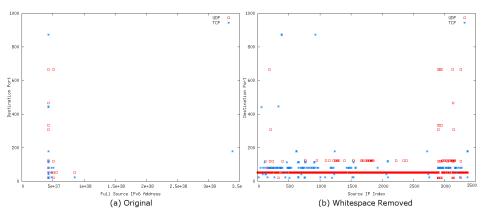
- Capture raw data Wireshark, TCPdump
- Parse Scripts in perl, python
- Process and reformat Nonexisting fields, size of data structures
- Display Designed for 32-bits



- The IPv6 address space is sparsely populated
- Vast majority of the address space is whitespace (darkspace)



- Why is visualizing the entire address space important?
- Remove whitespace
 - Keep a (sorted) list of the "seen" IPv6 addresses
 - When plotting, use the index rather than the full address
 - Optionally insert gaps between points



IPv6 Address Allocation

- IPv6 addresses must be allocated hierarchically
 - Avoid unnecessary load on backbone routers
 - Give greater meaning to IP addresses
 - Flexibility to organizations for block assignments
- RFCs that specify how addresses can be aggregated to keep routing tables efficient
- Reading more bits of an IPv6 address reveals more information (country, AS, ISP, zone, etc)
- Treemaps are useful for visualizing hierarchy

IPv6 Address Visualization with Treemaps

- Parse the dataset identifying all the unique IPv6 addresses
- Make each hextet a level of the tree
 - 2001:0DB8:0000:0078:9ABC:0000:0000:0000
 - 2001:0DB8:FABC:0078:9ABC:1234:5678:EEFF
- If there is more screen real-estate, display more hextets

IPv6 Address Visualization with Treemaps

- Improvements by color-coding type of traffic
- Make the size of each node proportional to the volume of data
- Display port number information in the contents of each node

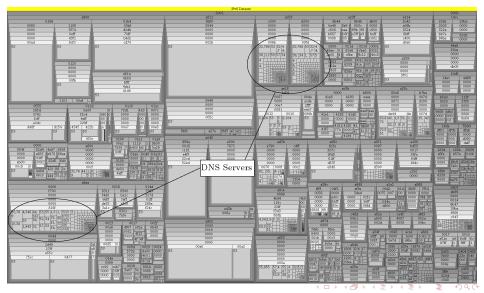
IPv6 Treemaps

	IFv6 Capture	
8800	3898 3811	2801 7222 7218
0000 4200	004d 0023 014d 014e 8bf0 0000 024f 7363 0009 2644 2646	9bc3 1395 950d 000b 870b 149e 5ce5 0591
0000	2149 0400 3271 0000 0000 0000 0000	7c93 15a4 93t0 9f96
0000 00 5906 2947 297a 6190 d	27ff 0000 01ff 000 2 0000 0000 0000 0000	54ff 19ff 06ff 25f ff22 a5d8 9669 32
0000 0006 003a 00af 0		1463 4f40 481d 7
	0000 0027 0000	
		9a05 9a59 9a2:
	6477 0018 0017 1019 0029	746a b3ff 025b 51c2 (051 a350
	22 14d0 163 4007 330 3 900	40x4 eefe 167d
2806 04/0 8229	8300 addr 00000 0004 0014 0	d884 5463
0068 0095 0065	2850 baic 8 6 572b 000 0015	aD05 1000 9000 9010 9023 0000
	atize atizi atizi	734b 99/0 09db 004e
	25e7 (500) 00e8 856a	6793 0086 0107 9ed8 a5 90 96 027 2000 2000 9e3 0 0 27
p	7290 7 0424 1292 4884 0018 0000 tb#p df85 0000 c181	5490 000 13 13 17
04:0 07:5 2324	0000 8387 5e02 0000 e4ff 0000 7c78 8537 0000 22ct	800d 120 1301 1 5400 913 330 6tg
28fc 00a3 0036 0004	0000 2200 000e 0135 046 0000 52ed	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
p	0508	0000
2909 200 2014	1276 4294 42 4294 42 4290 443	0000
45% 0000 004d 0002	7872 00	0000 0212 02fc 0286
0016	0002 9 1622 7 8049 9233 638 003: 0000 0000 fbs 0000 0000	0000 2211 e400 s211 6:50 8672 6134 0700
22a3 04c4 0766	0000 4338 10 101 1005 100 4233 0001 001 0000	0000 6995 5300 8774
000 0000	35eb	
60ba 0 822 0431	0000 1792 200 156 156 156 156 156 156 156 156 156 156	0201 0200 0200
0 0000 2895 0050 0000 0 5abd 0020 2895 0050 0000	13 00 1 2072 1 1 000 0000 000 1 0 1 1 0000 0000	This late booking in an
0000 0 2873	0000 3042 1b3e 1 02fe eCbs eSff	1 000 005 007 1 0 1 0 0 1 0 2 0 0 2 1 0 2
	0019 80%0 8259 307c 00d9 00dd 622c 005 0000 1524 0000 91d9 0000 d742	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
8001 5541 0200 5557 4202 c500 449 95aa 0000 0000 0000 9505 000 86c	0000 82ff 0000 61ff 0003 8335 wtbc	10 S 490 02 02 0
Seff 0000 0000	0000 0000 0000 0000 0000 0000 0000 0000 0000	200 1 202
107	53 53 63 651 651 652 622	0000 5484 5858
	5100 5500 2035 a177 a300 500 0144 1aa4 0000 5001 5022 0000 507 d200	6600 7bfc 8d55 b544 0000 0000
0156 01b4 011d 0555 0080 00bf 5600 8500 255d	68db 316c 3110 010 014f 000	53b0 0000 0000
0000 d2db 55c4 4a36 3762 0000 70ff 4eff (7d9 fcff	0523 00 00 + +++++++++++++++++++++++++++++	200e 5866 5cda
0000 b4dc 229f 9393 e2dc	000 000 000 000 000 000 000	6379 8000 5304
00ed 0070 434 422 4 mm3 d48f d135	8tf faff y64 0000 0000 0000 00000, 000000, 000000, 000000	0000
5000 6300 F	a100 4ecb ffff 00 a640 a540 a35c ca45 ef01 0000 0 a680 ff11 1 10 6c 04f1 4067	0000 bt14. 5329-07 2075 5569-8
0109 01ac 0100 0200	bd53 c201 000 000 120 17 0000 000	2402 2807
7341 0007c 0000 0002	001/ 1311 saits 0003 992f solt soit 337a cter	3a12 abid
1105 0120 0000 0000 00025 0041 0108	64ff 0000 0062 000 0062 000	0000 0000 004b 0017
0eff 0000 408d 000 4286 000 1000		
4171 0000 000 000 0110 4180 0000 0119 88800	2 0 4105 4101 415 41 sots 0000 001b	
53 4149 0107 0100 1119 9600	41 418 3d+4 9754 ad7a - orp 0 1 - c5 ac ag	2403 2ffre 2407 240 0400 022tt 2800 258
	4100 4112 7 418 0000 0011 0012 9999 42 82 800 442 1 122 4	00 0 C34 2005 24 1

IPv6 Hierarchy

Conclusions

IPv6 Treemaps



20/22

Conclusions

- IPv6 is here
- New visualization techniques/tools to support IPv6
- 2 proposals for dealing with these datasets

Introduction	IPv4 vs IPv6	Problem	Whitespace Filtering	IPv6 Hierarchy	Conclusions
Questic	ons				