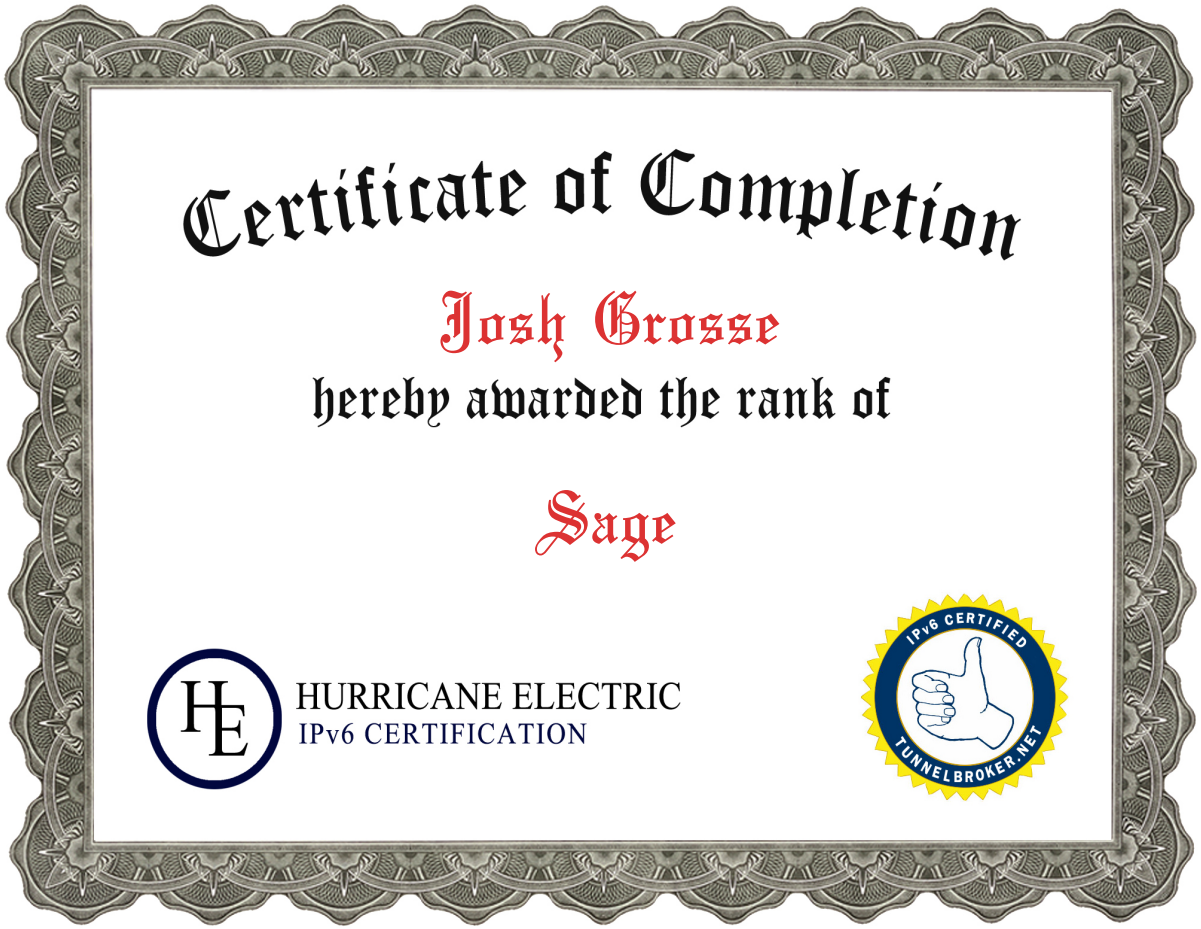
IPv6 for the Vaguely Aware

Josh Grosse

SemiBUG - April 18, 2017

I did it

- You can too



Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Retained from IPv4

These remain the same - Mostly

- The TCP and UDP protocols
- Reverse domain name resolution (address -> name) via PTR records

Dropped from IPv4

But they're not really gone

- Netmasks
  - We don't provision them, we use prefix lengths
  - Used internally by the IPv6 network stack
- NAT
  - Unnecessary for IPv6 traffic
  - NAT64: common mechanism for IPv4/IPv6 translation
- DHCP
  - Not strictly necessary
  - Has use-cases such as nameserver address provisioning - as in IPv4
  - ISPs may use it for subnet allocations ("DHCPv6 Prefix Delegation")

Revised, conceptually identical

The more things change, the more they change the same

- Address notation: “dot decimal” -> “colon hexadecimal”
- CIDR notation -> “prefixlen” or “prefix length” or “prefix”
- DNS: A -> AAAA records
- Private addresses -> “Unique Local Addresses” (fd00::/8)
  - Not addressable on the Internet
  - Internet addresses are “Globally Unique”
    - *A maze of twisty little passages, all different.*

Replaced, and conceptually different

These take some getting used to

- ARP -> Neighbor Discovery Protocol (NDP)
  - LAN (Neighbor) address resolution, like ARP, plus:
    - Discovery
    - Conflict resolution / elimination
    - Stateless Address Autoconfiguration (SLAAC)
    - Routing (both soliciting and receiving router advertising)
- ICMP -> ICMP6
  - Required - used for NDP and other critical info
  - You can block ICMP and much of IPv4 will still work
    - Not perfectly, but it will still (mostly) function
  - Blocking ICMP6 will *break* IPv6
- Broadcast -> Multicast
  - Multicasting is part of NDP
  - 224/4 -> ff00::/8

Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Conceptually similar, yet different (1 of 3)

Similar, but then it goes sideways

- The standard subnet is a /64 prefix
- This is *the* standard subnet delegation – SLAAC requires it
- Recall: an IPv4 /24 subnet with a 32-bit address
  - The first 24 bits defines the subnet
  - The last 8 bits defines the device address on the subnet
- So an IPv6 /64 subnet on a 128-bit address:
  - The first 64 bits define the subnet
  - The last 64 bits defines the device address on the subnet
- But the number of bits used makes a difference
  - A *vast* difference

Vastness (2 of 3).

- /64 subnets are passed out like candy at Halloween – they got lots and lots
  - My ISPs both gave me /64s *for free*
  - In comparison, one charges $24/year for a 2nd IPv4 address
  - The other doesn't even *offer* a second IPv4 address
- What do I get with one little /64?
  - 2^{64}addresses
  - That's **18,446,744,073,709,551,616** addresses
  - Hoo boy, that's a lotta commas.
    - Let's experiment with the vastness of a standard /64
    - We'll use Spam, because everyone *loves* Spam

Experimenting with Spam (3 of 3)

Not really - just for a thought experiment

- According to published press reports citing a Radacti Group study
  - 205 Billion Emails were being sent daily in 2015
  - 49.7% of that traffic was identified as Spam
- Let us assume this was and is still true, and thus, for our experiment:
  - 101.8 Billion Spam Emails are sent each and every day
- And, as this is our experiment:
  - All spammers share a single /64 subnet
  - Each Spam Email gets a use-once IP address, that is never used again.
- How long will it take to go through all IP addresses in the /64?
  - More than 496,114 years: “polynomial time”

Link-Local Addresses

You can use it FOR routing but not IN routing

- Required, used with NDP
- Every NIC gets one (fe80::/10)
- Locked to the NIC:
  - Embeds the MAC address
  - The interface name *must* be appended to a link-local address
  - Commands and interface names vary by OS, but all link-local addressing requires it:
    - ping6 fe80::f23f:eb0d:21af:7c39%em0
- Local to the broadcast domain (LAN) and cannot be routed
- Used as next-hop addresses in routing tables

Autoconfiguration Privacy

This is completely new

- Expect a NIC to have multiple IPv6 addresses.
  - There is the Link-Local address
  - There may be static addresses
  - There may be automatically assigned addresses
- Automatic addresses may be random and temporary.
  - *Without* privacy, automatic address assignments contain the MAC address
  - *With* privacy, these addresses are random
- Autoconfigured addresses are temporary
  - New address assignments may be as infrequently as once-per-boot, or as frequently as configurable by OS and admin
  - Address lifespans may overlap, as replaced addresses are *deprecated* before deletion

Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Live Demo

Live Demo

Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Have you got a little list?

From www.jeliza.net, author unknown

Then there's evil Spamford Wallace and his Cyberpromo slime–

*The e-mail terrorist– I've got *him* on the list!*

With his unrepentant attitude and arrogance sublime,

*It's easy to insist– he *must* be on the list.*

He harvests our addresses, which he sells to other jerks

Then he spams us selling software we can buy to block their works.

New domains most every day, a tough man to ignore,

Send him a "Remove" request, he only spams you more.

He wants to make a profit, doesn't care how much he's dissed.

*But I don't think he'll be missed– I'm *sure* he'll not be missed!*

IP list considerations

"(Because your mess) your mess is on my list" - not Hall & Oates

- In IPv4, it's relatively easy to maintain reputation lists to:
  - Block incoming traffic (Blocklist / Blacklist)
  - Permit incoming traffic (Whitelist)
  - Temporarily block the traffic to assess it (Greylist)
- Those lists can include network blocks and individual addresses
- In IPv6:
  - We can whitelist
  - We can greylist (when possible and useful)
  - Blacklisting must change:
    - IP addresses will be random and temporary
    - We can't track and manage individual addresses in Carl Sagan quantities

Blacklists / Blocklists

Block the /64s

- Move from blocking individual address to blocking subnets
- Same general mechanics as the IPv4 lists.
- Prefix blocking will be mandatory for attack mitigation
- Positive - there is much less to block (for now):
  - The"Script kiddie" brute-force scan / attacks require polynomial time.
- Negative - a /64 may be too broad in some situations, causing collateral damage

Whitelists
Similar to IPv4

- Individual address must be static.
- Whitelisting /64s may introduce new types of trust

Greylists
Current tech could apply

- A greylist is a connection placed on "hold" until a test is passed:
  - "Verify, *then* trust" - R. Reagan's ignored advisors
  - success = whitelist
  - failure = blacklist or return to greylist
- Examples:
  - EMail confirmation link - prove an Email address worked
  - CAPTCHA test - prove that a human is involved (hopefully)
  - EMail transfer deferrals - prove a sending Email server might be real and not a Spambot (hopefully)
- Problems:
  - Greylisting requires admin oversight and may also require admin and compute overhead
  - Some applications may not have a useful "test"
  - Some solutions may not scale sufficiently

Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Infinite IP addresses

Finite, but *effectively* infinite.

- The game of whack-a-mole with individual IP addresses does not exist
  - Randomized, changing IP addresses are baked right in
- As with IPv4, broad spectrum blocks may further an attacker's aims
- Greylisting may be an imperfect solution
- Without brute force scans, expect new attack vectors:
  - Harvested addresses in AAAA records (DNS)
  - Harvested addresses from traffic (sniff!)

Outline

1. 1. How to survive IPv6
   - IPv4 Concepts in an IPv6 World
   - New concepts in IPv6
   - Examine a production server (demo)
2. 2. Be a criminal mastermind - thrill your friends!
   - IP Reputation Lists
   - The criminal's advantage
   - Fighting back
3. 3. Getting started

Should you worry about IPv6 Black Hats?

Yes

- They exist
- Otherwise, lists like this would not be needed
  - The Spamhaus DROP (Don't Route Or Peer) lists are advisory "drop all traffic" lists, consisting of netblocks that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers). The DROP lists are a tiny subset of the SBL, designed for use by firewalls and routing equipment to filter out the malicious traffic from these netblocks.

    ; Spamhaus IPv6 DROP List 2017/02/03 - (c) 2017 The Spamhaus Project
    ; https://www.spamhaus.org/drop/dropv6.txt
    ; Last-Modified: Sat, 31 Dec 2016 22:34:51 GMT
    ; Expires: Fri, 03 Feb 2017 20:07:00 GMT
    2a07:5807::/32 ; SBL300884
    2a06:2a00::/29 ; SBL310268
    2a06:e480::/29 ; SBL301771
    .
    .
    .

What's the solution?
Defenses in depth

- The script kiddies are gone for now - until more complex and intelligent scripts are devised
- VPNs mitigate address harvests from traffic.
- Private (non-authoritative) DNS for private services may mitigate AAAA record harvesting
  - But public (authoritative) DNS is public by design.
- Use whitelist when you can (as with IPv4)
- Use a greylist when you can (as with IPv4)
- Block /64s as necessary, but ...
  - Block or Not?
    - A /64 in a cable customer netblock
      Comcast IP Services, L.L.C. MICHIGAN-RPD-V6-2 (NET6-2601-400-1)
      2601:400:: - 2601:43F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    - A /64 at a cloud services provider
      Vultr Holdings, LLC NET-2001-19F0-5C01-48 (NET6-2001-19F0-5C01-1)
      2001:19F0:5C01:: - 2001:19F0:5C01:FFFF:FFFF:FFFF:FFFF:FFFF

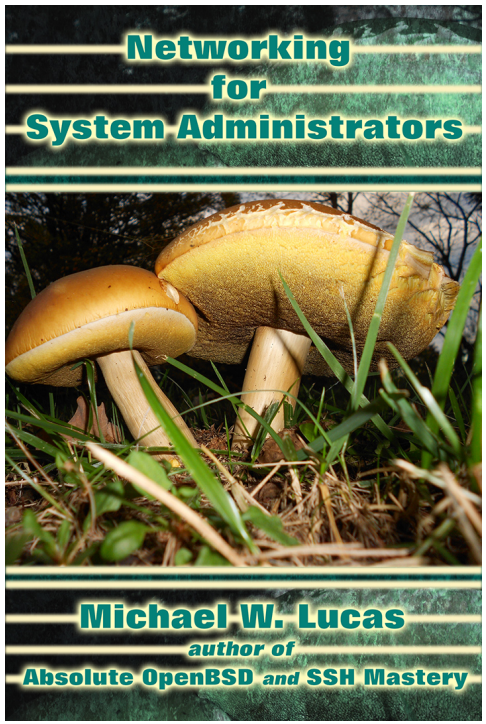
Abuse management

- Consider the nature of the abuse, and the application mix and purpose
- Situational blocking may be helpful - 3 examples:
  - Spam:
    - "Let's block SMTP, but keep web services open so they can complain."
  - Security threat:
    - "Terminate that /64, and LART their ISP's abuse@ maildrop."
  - DDOS:
    - "Block that continent. Heck, block that hemisphere, *then* call the CIO. With her, it's easier to get forgiveness than permission."
- Can you take the time to conduct an analysis before blocking?
  - "Shoot-first, forget to ask questions later!"
- Are you willing to *communicate* with an Abuse Desk, and not just LART them with Email or a web form?

Getting Started

This was invaluable for me

- After a 2 decade hiatus, this was my reintroduction to IPv6
- It contains OS-agnostic advice and guidance
- ISBN-10: 0692376941 ISBN-13: 978-0692376942



- *Disclaimer: I know the author*