IPv6: How to Securely Start Deploying!

Fundamentals

Joff Thyer © 2020

Agenda

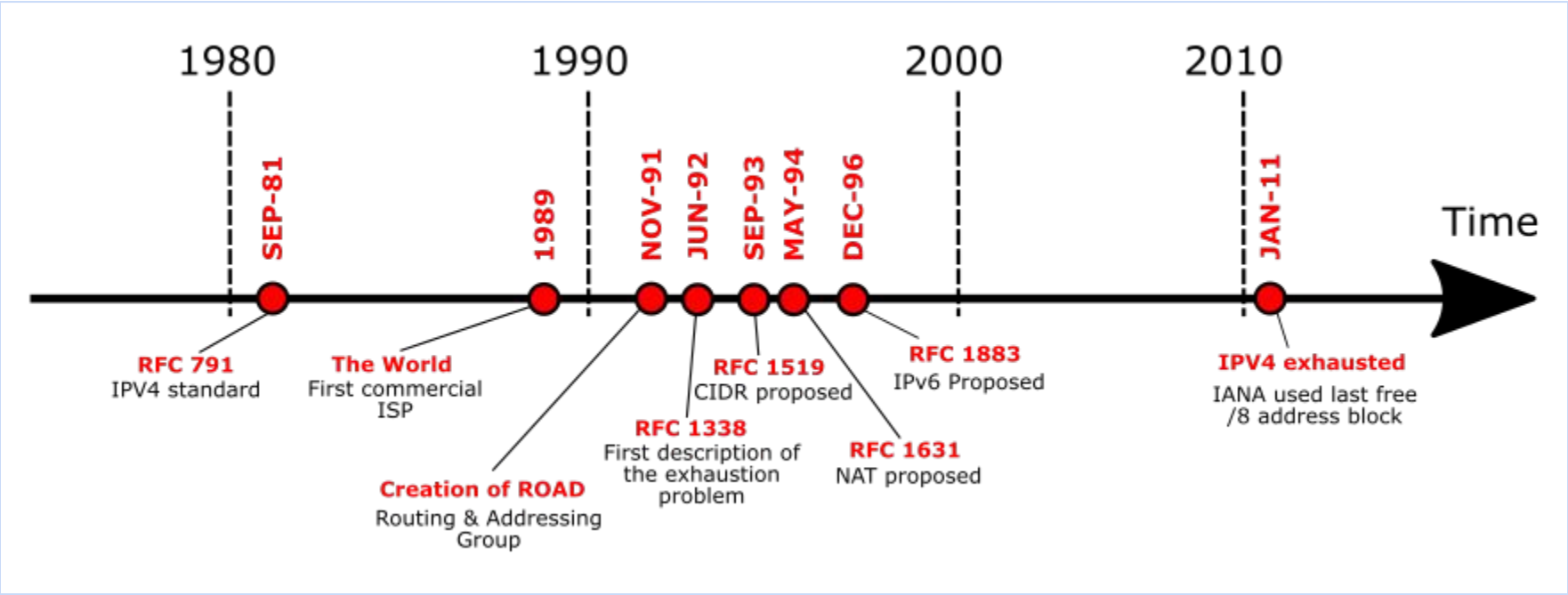
- Joff Thyer (@joff_thyer)
  - Black Hills Information Security
  - Security Weekly Co-Host
  - SANS SEC573 Certified Instructor

- Agenda
  - Why do this? / Goodbye v4.
  - IPv6 Fundamentals
  - Securing the v6 things
  - Misc Fun Discussion

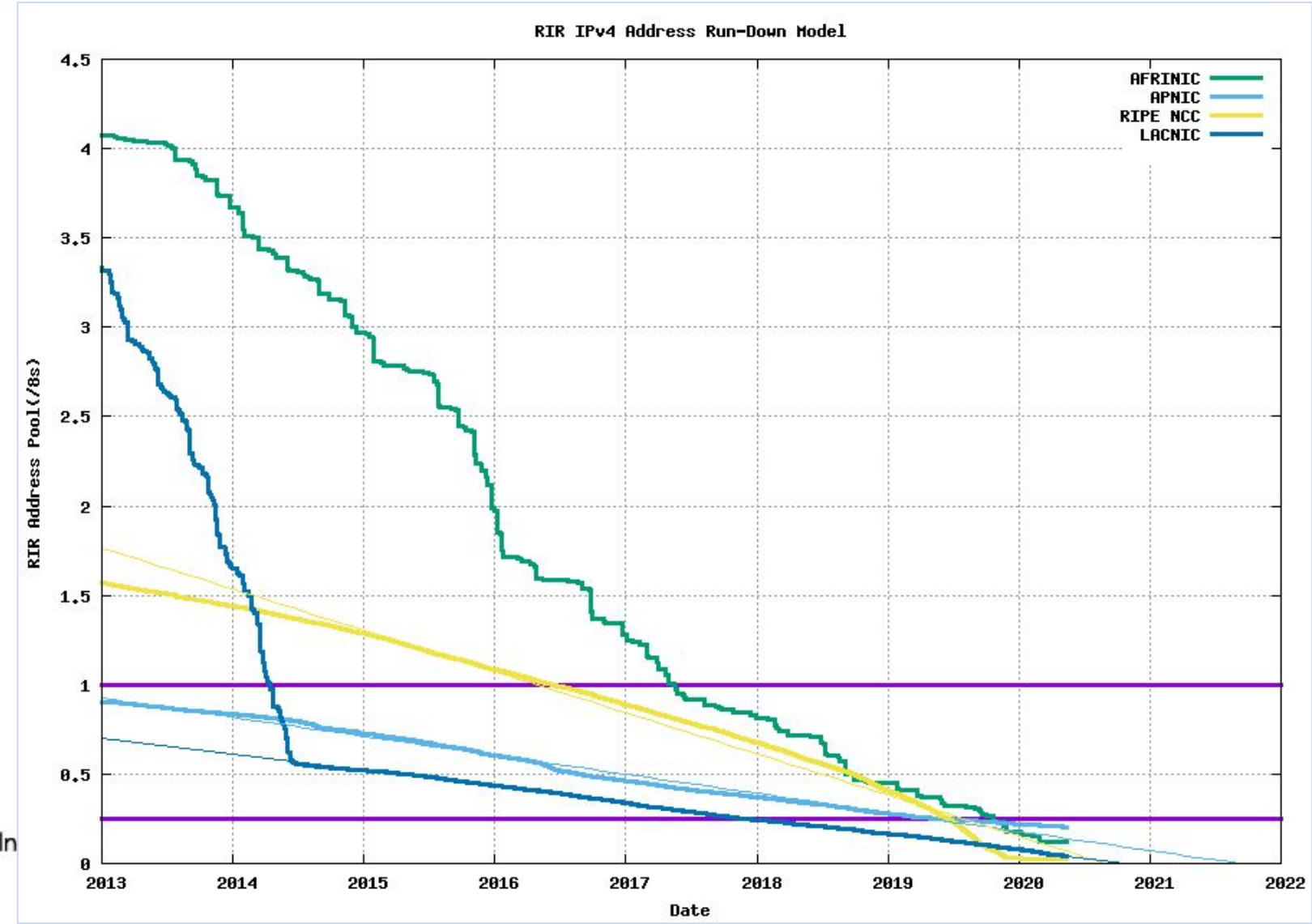
Why do this?

- The IPv4 protocol was designed in the 1970's.
  - We ran out of numbers! (well sort of..)
- IPv6 gives us
  - More than adequate address space
  - Eliminates bolt on protocols (ARP)
  - Remedies global route table disaster
    - Yes CIDR is cool but the resource impact hurts.
- Myth buster!
  - Not more or less secure that v4
  - Just different.

IPv4 Timeline



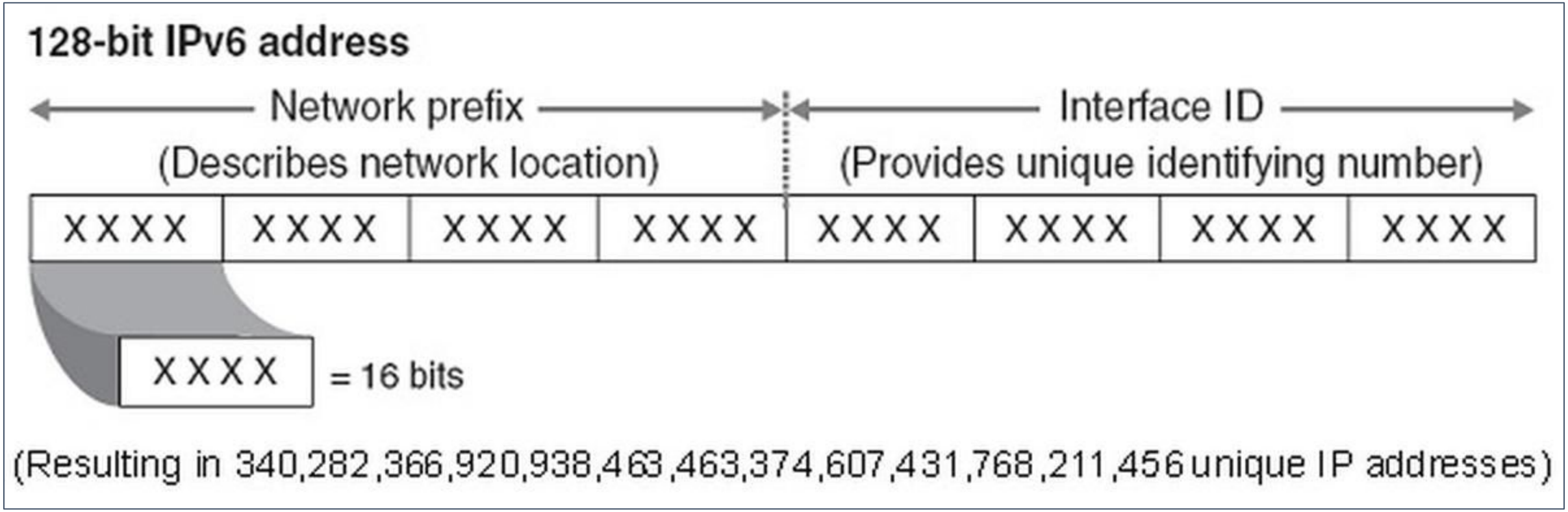
RIR Allocations?



The IPv6 Address

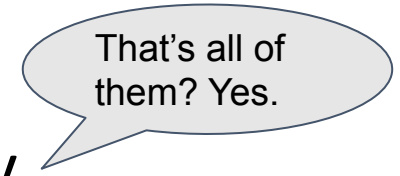
- 128-bit addresses!
  - 2 ^ 128 = a very large number
- Address is expressed as hexadecimal rather than dot quadded decimal.
  - 8 groups of four hex digits
    - leading zeroes can be omitted.
    - multiple groups of all zeroes can be omitted (compressed)
- Example unicast addresses:
  - 2001:0410:0009:0479:0000:0000:0000:0001
  - 2001:410:9:479::1 ← short form of the same address

IPv6 Address Format



Where did IPv5 go?

IANA Allocated IPv6 Blocks



- There are a total of 35 address blocks allocated today
  - 7 x /12 : various RIR's
  - 1 x /16 : 2002::/16 for 6o4 translation
  - 1 x /18 : RIPE-NCC
  - 2 x /19 : RIPE-NCC & APNIC
  - 3 x /20 : RIPE-NCC & APNIC
  - 3 x /22 : RIPE-NCC
  - 18 x /23 : various RIR's

- /12 means 12 network bits (128 -12 = 116 bits)

IPv6 Packet Encapsulation

- Ethernet protocol type 0x86DD
- Can be tunneled within IPv6 using protocol 41.
  - Known as 6 in 4. Probably *already* operating on your network!
- Mapping of Ethernet address to IPv6 address requires ICMPv6
- ICMPv6 uses Multicast for Neighbor and Router Discovery functions.

- Bottom line:
  - Broken multicast == Broken/DoSed network.
  - You want DoS? Then spray out packets to tons of Ethernet multicast destinations and kill switch TCAM.

IPv6 Address Types

- Three different types of address
  - Anycast
    - same address assigned to more than one host interface.
    - Packets routed to anycast will arrive at nearest (shortest route) host.
  - Unicast
    - Single address assigned to a host interface.
  - Multicast
    - Defines a group of devices interested in receiving traffic via this address.
- There is no such thing as broadcast packets in IPv6!

IPv6 Address Scopes

- Unicast / Anycast addresses can have two scopes
  - Link-local scope
    - Only to be used on a single directly attached network link
      - Must exist because … “NO BROADCAST!”
    - Prefix is: **FE80::/10**
  - Global scope
    - Globally routable address
- Multicast addresses scope is defined by 4 least sig. bits in second octet
  - Address format “**FF0s::**” whereby the “**s**” defines the scope
  - Numerous pre-defined / well known multicast scopes

IPv6 Multicast Scopes

- Predefined scopes (FF0**s**::):
  - FF00:: reserved / unused
  - FF01:: interface local / host bound
  - FF02:: link local
  - FF03:: realm local
  - FF04:: admin local
  - FF05:: site local
  - FF08:: organization local
  - FF0E:: global
  - FF0F:: reserved / unused

IPv6 Address Assignment

- How does an endpoint get an address?
  - Stateless Address Auto-Configuration (SLAAC)
  - DHCPv6
  - Combination of DHCPv6 and SLAAC
  - Static Assignment

- Things to consider.
  - The host identifier portion of an IPv6 address is the lower 64 bits
    - /64 sub-networks will be commonly deployed
    - /64 = 1.844×10^{19} addresses!
  - All interfaces have to generate a link-scope local address within “fe80::0/64” (RFC4291)

IPv6 Multiple Interface Addresses!

- Your network interface can have addresses for
  - Link-local scope
  - Site-local scope
  - Unicast global scope - possibly many addresses
- Suggested benefits (RFC 7934) include:
  - Virtual machine use
  - Per-processor addressing
  - Per-application addressing (micro-app flows..)
  - Dual stack v4/v6 translation mechanisms
  - Privacy addressing

IPv6 EUI-64

- Applies to both SLAAC global and link-scope local addresses
- An Ethernet/MAC address is 48 bits
- To construct the IPv6 address, we follow this recipe
  - Split the 48 bits into two 24-bit components
  - Insert 0xFFFE in between the two components
  - Flit the seventh most significant bit (from the left) for universal scope
- Example addresses on a Linux interface

```
inet6 2001:470:7:379:2e0:4cff:fe68:c1  prefixlen 64  scopeid 0x0<global>
inet6 fe80::2e0:4cff:fe68:c1  prefixlen 64  scopeid 0x20<link>
ether 00:e0:4c:68:00:c1  txqueuelen 1000  (Ethernet)
```

ICMPv6

- Header has same structure as ICMP in v4.
- ICMPv6 and Multicast are essential for IPv6
- Four categories
  - Error Messages
  - Informational Messages
  - Neighbor Discovery Messages
  - Other ICMPv6 Messages

- Proper infrastructure security means that you must defend/protect/filter both ICMPv6 and Multicast.
  - It’s your V6 protocol control plane!

ICMPv6 Error Messages

- Type 0: Reserved/Unassigned
- Type 1: Destination Unreachable
  - Code 0: No route to destination
  - Code 1: Administratively prohibited
  - Code 2: Unassigned
  - Code 3: Address Unreachable
  - Code 4: Port Unreachable
- Type 2: Packet Too Large (used for Path MTU Discovery)

ICMPv6 Error Messages …

- Type 3: Time Exceeded
  - Code 0: Hop (TTL) Exceeded
  - Code 1: Fragmentation reassembly time exceeded
- Type 4: Parameter Problem
  - Code 0: Erroneous header type
  - Code 1: Unrecognized header type
  - Code 2: Unrecognized IPv6 option encountered
- Types 5 - 127: Reserved/Unassigned

ICMPv6 Informational

- Type 128: Echo Request
- Type 129: Echo Reply
- Type 130: Multicast listener query
- Type 131: Multicast listener report
- Type 132: Multicast listener done

ICMPv6 Neighbor Discovery

- Type 133: Router solicitation
- Type 134: Router advertisement

Like DHCP that gives route/DNS info only.

- Type 135: Neighbor solicitation
- Type 136: Neighbor advertisement

Similar to ARP but over Multicast

- Type 137: Redirect

Sigh :(

- Types 138 - 161: Assigned by IANA for various purposes
- Types 162 - 255: Reserved/Unassigned

Define “reserved” please….

ICMPv6 ND is Analogous to ARP

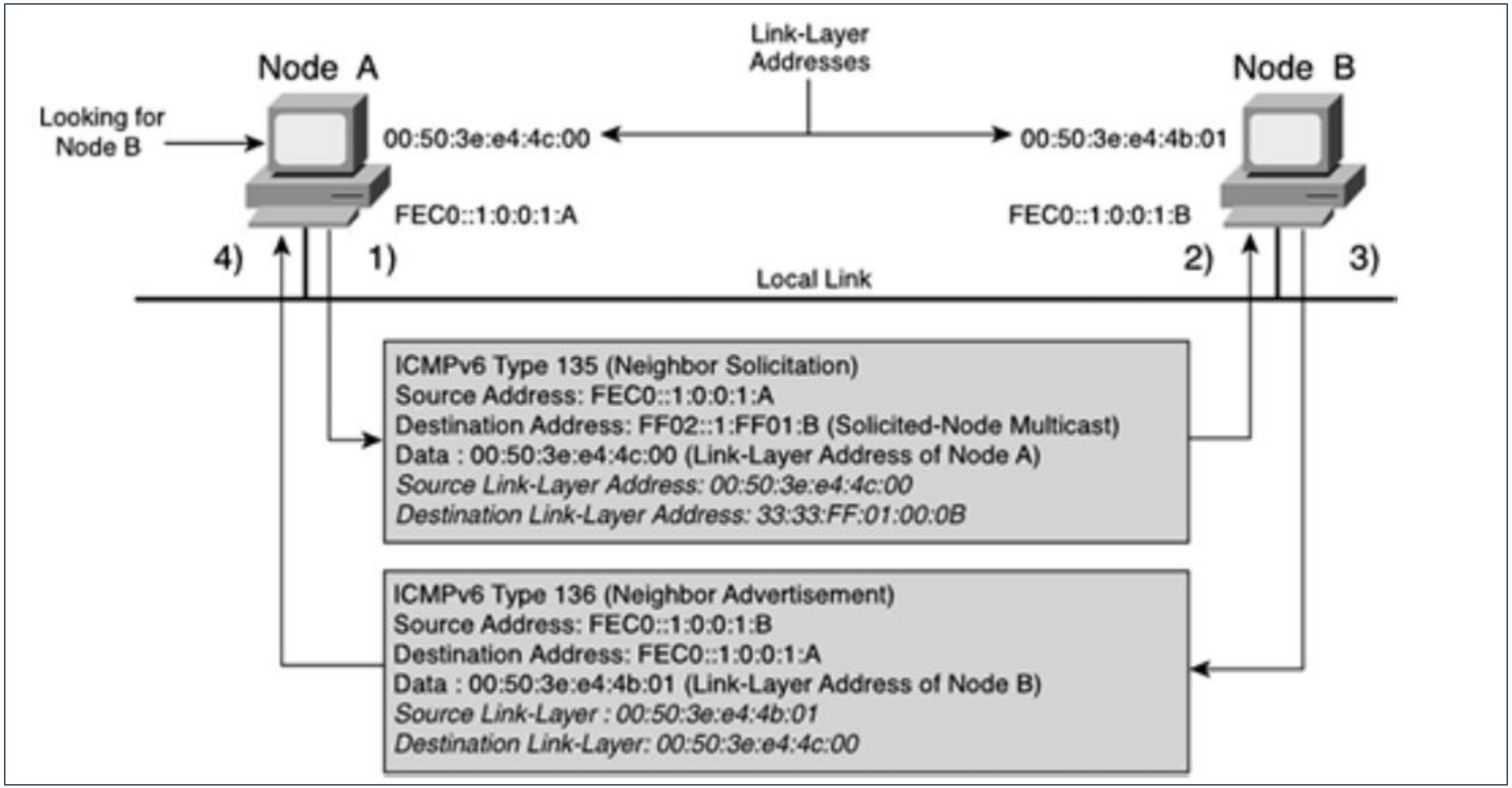


Diagram from community.cisco.com

Securing the v6 things..

IPv6 Perimeter Security

- Areas of concern include:
  - Address filtering
    - Allocated addresses
    - Anti-spoofing
  - ICMPv6 filtering
  - Multicast filtering
  - Protocol normalization
  - Privacy / Obscurity, and Route Tables
  - Other..

IPv6 Address Filtering

- Return of the bogons!
- A LOT of IPv6 is unallocated space.
- You should filter appropriately.

- Don't allow a packet sourced from ANY unallocated address enter your network.

IPv6 Address Filtering …

- Implement Anti-Spoofing perimeter ACL:
  - No packet with a source address of your network allocation can ENTER your network.
  - No packet with a destination address of your network allocation can LEAVE your network.

ICMPv6 Perimeter Filtering

- Two categories of traffic
  - Traffic *initiated* from perimeter security device
  - Traffic that is *in-transit* across perimeter

- *Transit Traffic* Category Recommendations
  - Start with a DENY ALL approach, and then allow selectively
    - Ensures that all unassigned/experimental types are DROPPED.
  - Allow Type 1: Destination Unreachable
    - Filter selectively allowing only specific codes such as code 4 - port unreachable.
  - Allow Type 2: Packet too large. (Do not break path MTU discovery)
  - Allow Type 3, Code 0 only. (TTL/Hop limit expired)
  - Allow Type 4, Codes 0 and 1 only related to header errors.

ICMPv6 Filtering - Transit Traffic

- Transit traffic filtering continued…
  - Optionally allow ICMP types 128/129 (echo request/reply) based on local ICMP security policy.
  - Allow ICMP types 144 through 147 ONLY if your IPv6 network is “mobility enabled”. Many may choose to leave this in default drop state.
  - Optionally allow ICMP Multicast related messages (types 151 - 153)
    - ONLY applicable if you participate in global multicast sourcing.

- ICMP type 137 (Redirect) represents a direct security threat and should always be dropped at the perimeter.

Surprised?

ICMPv6 Filtering - Non-Transit

- Traffic initiated from perimeter security devices
- Again start with a DENY ALL policy
- Use the same recommendations as transit above with the exception of the mobility enabled class
- Additional messages to ALLOW should be:
  - Types 133/134: Router solicitation / advertisement
  - Types 135/136: Neighbor solicitation / advertisement
  - Types 141/142: Inverse neighbor solicitation / advertisement

IPv6 Multicast Filtering

- Be careful to distinguish perimeter from internal network
- ICMPv6 works hand-in-hand with Multicast
- This means…
  - Neighbor discovery has to function internally
  - Router discovery has to function internally
  - End hosts should NOT be permitted to advertise as routers
  - End hosts should NOT be gratuitously responding to neighbor solicitation

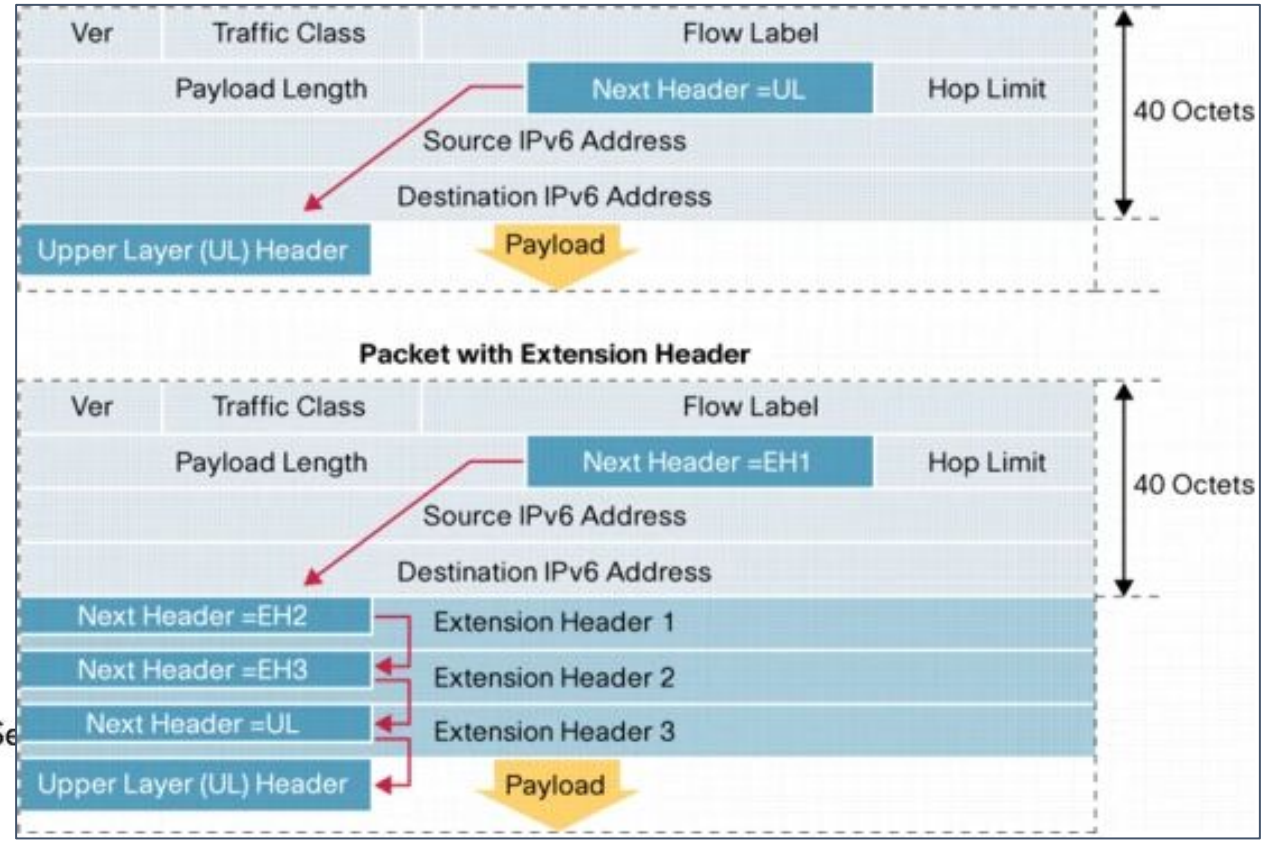
- Perimeter network devices may well need to use neighbor discovery mechanisms but such traffic should NOT transit the perimeter.

IPv6 Multicast Filtering

- Likely assumption for most is to <u>not participate</u> in global/inter-domain multicast
  - Any packet with a multicast source address should be dropped
  - Reserved and unused multicast destinations should be dropped.
  - Probably most other multicast destinations will be blocked in a perimeter context.
    - You don't want any site or organization local traffic crossing the perimeter
    - Realm-local scoped traffic will be confined to specific technologies.
    - The decision to drop realm-local will have to be policy based.
  - Global multicast should be dropped if not participating inter-domain.

IPv6 Protocol Normalization

- IPv6 has a protocol header field labeled “Next Header”.
- Normal OSI Layer 4 headers are called an “Upper Layer Header”
  - There can be chained “Extension Headers” in the frame before UL Header.



IPv6 Extension Headers

Danger Ahead!

Protocol Number	Description	Reference
0	IPv6 Hop-by-Hop Option	[RFC8200]
43	Routing Header for IPv6	[RFC8200][RFC5095]
44	Fragment Header for IPv6	[RFC8200]
50	Encapsulating Security Payload	[RFC4303]
51	Authentication Header	[RFC4302]
60	Destination Options for IPv6	[RFC8200]
135	Mobility Header	[RFC6275]
139	Host Identity Protocol	[RFC7401]
140	Shim6 Protocol	[RFC5533]
253	Use for experimentation and testing	[RFC3692][RFC4727]
254	Use for experimentation and testing	[RFC3692][RFC4727]

IPv6 Enforcing EH Rules

- The rules to process extension headers are as follows:
  - Each extension header should NOT appear more than once except the destination options header.
  - The Hop-By-Hop options header (proto #0) should be the first header in the list
  - The destination options header (proto #60) should be at the END of the list and appear at most twice
  - The fragment header (proto #44) should not appear more than once in the list

- Umm…. so do we generally follow the rules?

IPv6 Header Normalization

- This area will continue to be a source of attacks.
- Normalizing and Filtering might can be subject to DoS attacks.
  - I will make your filtering device work really hard!
- Hop-by-Hop and destination options can including padding to 8-octet boundaries
  - Covert channel time!
- The Route Options Header (43) is similar to IPv4 strict-source/loose-source routing.
  - Send me all the things!

IPv6 Routing Header (RH0) Attack

- Routing Options Header (#43) with Source Route Type (#0) contained within is deprecated, because…
  - https://tools.ietf.org/html/rfc5095

  - The same IP address can be expressed multiple times in the header.
  - A packet oscillation and amplification can be arrange between two nodes on the network
  - Leading to… DoS or a DDoS cluster futz.
  - Why carry forward source routing into v6?

IPv6 Protocol Normalization

- These extension headers give operational flexibility and will be an ongoing source of security concerns
- Why? Because you can keep on developing new things to break and get broken.
- Recommendations:
  - Perimeter security devices must enforce the extension header rules
  - Perimeter security devices must have flexibility to filter not only specific header types, but subtypes within the header
  - If there is padding within any extension header that is NOT initialized to zeros, drop that packet!
  - Drop any reserved, undefined, and experimental extension headers.

Address Privacy / Obscurity

- Assume
  - An organization chooses a common vendor for endpoints (say Intel)
  - You can narrow down 24-bits of the MAC address to a subset of Intel OUI's.
    - A single Intel OUI would be **0013E8**
- EUI-64 link local address (default) is 100% reachable for ALL machines in that sub-network
  - FE80::213:E8FF:FEXX:XXXX
  - Leaves a 24-bit search space to find a neighboring node.
- SLAAC uses the same EUI-64 mechanism!
  - Know the subnet, then you know the Unicast global addr.
- And then there's this:
  - ping6 -i eth1 ff02::1

RFC4941 Privacy Extensions

- Recommended to enable this (ie: disable EUI-64)
- If so, the link local state address will be randomly chosen instead of using EUI-64
- With SLAAC, you will be granted another global unique address that will also be randomly chosen in the /64.
- In both cases, the duplicate address detection algorithm will run.

Endpoint Route Table

- Route table will be populated by ICMPv6 Router Advertisements
- Any endpoint could advertise a route!

- Infrastructure must be configured to block any ICMPv6 router advertisements from non-authorized sources
  - Ie: Block from all but the legitimate router(s)
- Be careful, don't block neighbor discovery / advertisement or you break the network.

IPv6 and NAT66

- There is a thing called NAT66 /Network Prefix translation.
  - Arguably we don't need it… ("vi" rocks)
- Things to consider:
  - NAT was designed to conserve addresses.
  - NAT happens to provide some address obscurity.
  - Stateful firewalling and application traffic inspection does not require NAT
- Having address independence may be a use case
  - https://tools.ietf.org/html/rfc6296

Summary Recommendations

- Implement anti-spoof, multicast, and bogon filtering at the perimeter
- Filter/control ICMPv6 traffic both at perimeter and within LAN
- Don’t allow bogus ICMPv6 Router Advertisements from end nodes
- Enable privacy extensions (disable EUI-64)
- Assign addresses randomly within the *sizable* sub-networks
- SLAAC is really more of an ISP than Enterprise Org thing.
- Don’t use NAT66 unless you really need addressing independence
- Minimize your (D)DoS Risk by:
  - Choosing perimeter security devices that can normalize protocol extension headers properly.
  - NOT trunking your VLAN’s everywhere or your network will die a horrible multicast switch CAM death.

Resources

- https://www.apnic.net/community/ipv6-program/ipv6-bcp/
- https://blog.apnic.net/2019/03/18/common-misconceptions-about-ipv6-security/
- https://bgp.potaroo.net/index-v6.html

- https://tools.kali.org/information-gathering/thc-ipv6
- https://tools.kali.org/stress-testing/ipv6-toolkit

- Book: IPv6 Security by Scott Hogue (Cisco Press)

Coming soon …

- We need real hands on, so how about these topics:
  - How to Build your own IPv6 Testbed Network
  - Leveraging IPv6 Security Tools for Fun and Profit
- Twitters: @joff_thyer
  - *I need more followers than Tim Medin*!
- Final thought: Dual IPv4/IPv6 stack sucks.
  - Twice the work, half the fun.