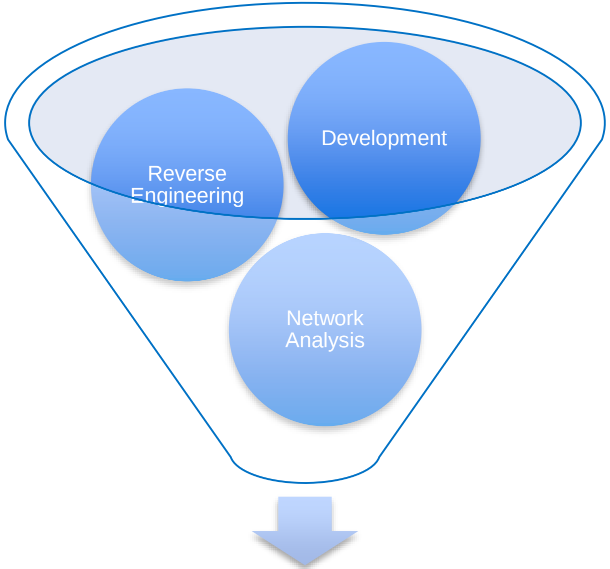
::1 The Official Home for IPv6 Attacks

Ronald Eddings , Marco Figueroa, Josh Porter

Information Technology

Who We Are



IPv6 Framework and Modules

Why We Are Here

IPv6 Refresher

What Is IPv6

Why We Must Switch

IPv6 can support 3.4 x 1038 or340,282,366,920,938,463,463,374,607,431,768,211,456 unique IP addresses.

Autoconfiguration support

Built-in IPsec

Additional support for real-time delivery of data

Advantages

Simplified packet header

Larger payloads

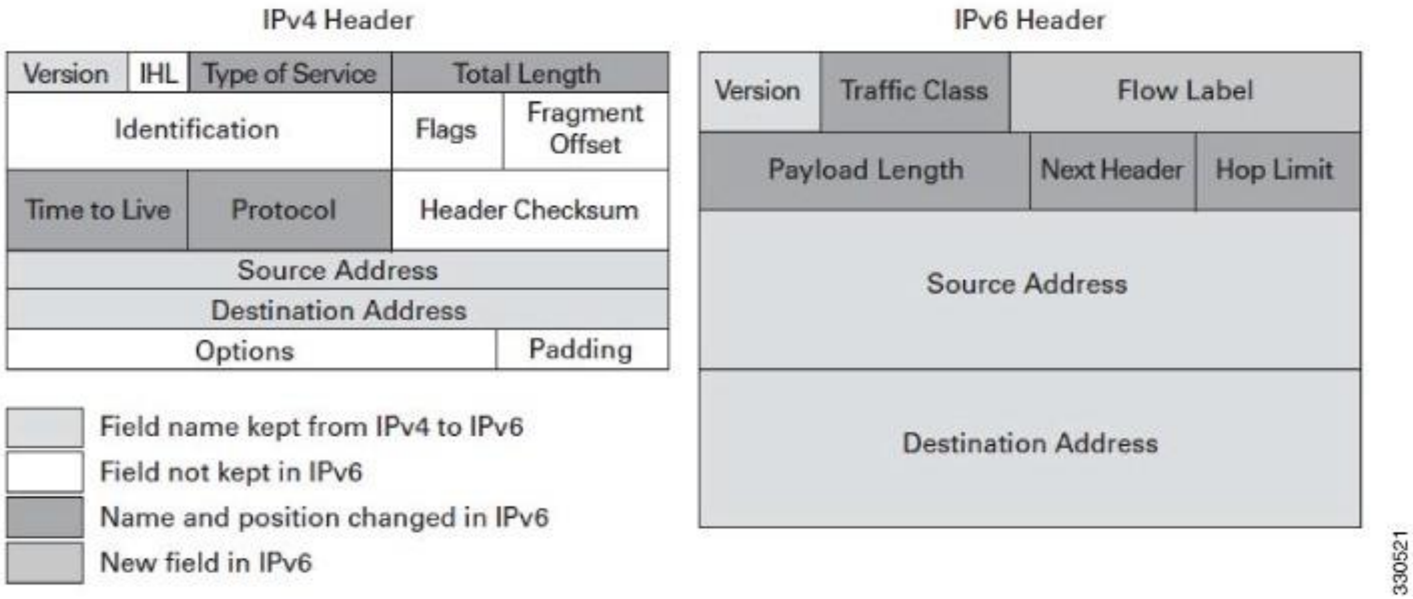
Auto configuration

Can potentially eliminate NAT

Increased number of multicast addresses

Support for preexisting routing protocols

IP Header Comparison



IPv4 Header

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

IPv6 Header

Version | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source Address

Destination Address

▨ Field name kept from IPv4 to IPv6

□ Field not kept in IPv6

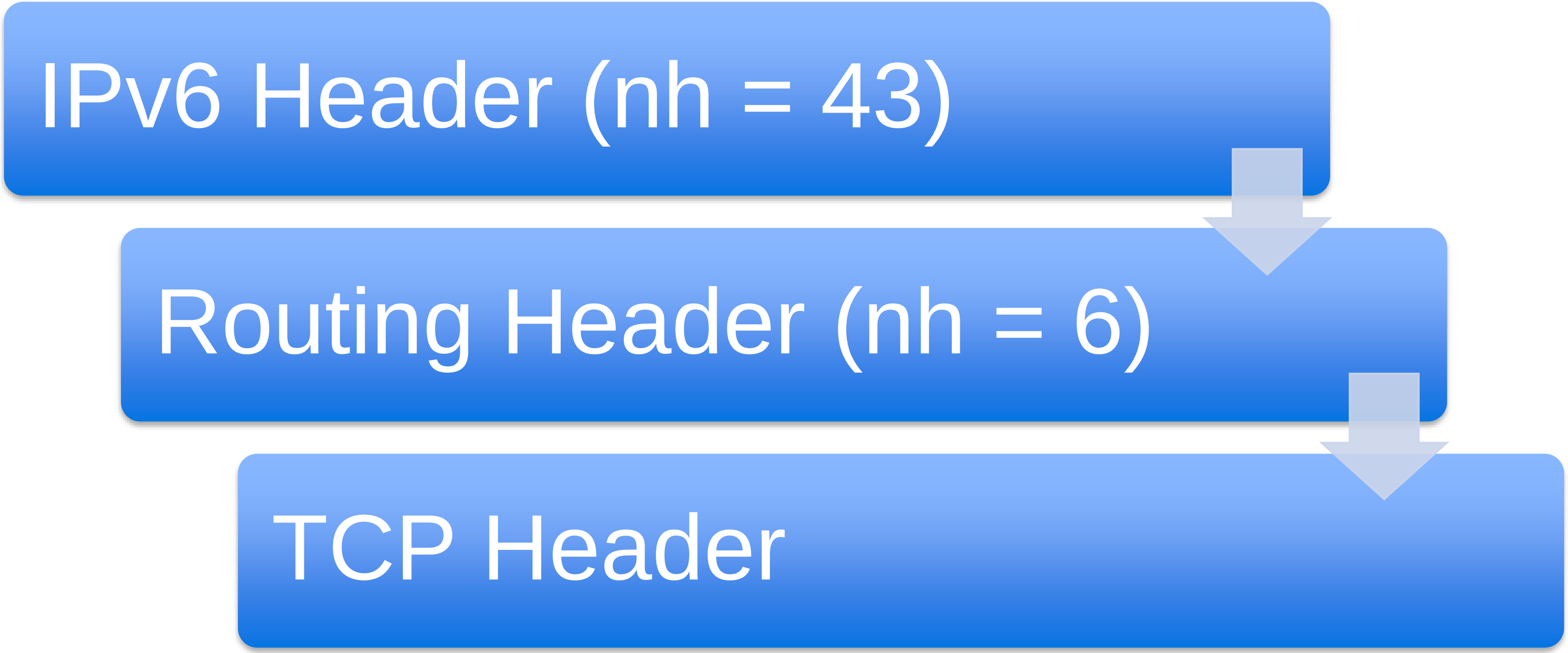
■ Name and position changed in IPv6

▩ New field in IPv6

IPv6 Extension Headers

Header Type	**Next Header Code**
Basic IPv6 Header	-
Hop-by-Hop Options	0
Destination Options (with Routing Options)	60
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulation Security Payload Header	50
Destination Options	60
Mobility Header	135
No next header	59
TCP	6
UDP	17
ICMPv6	58

IPv6 Extension Headers

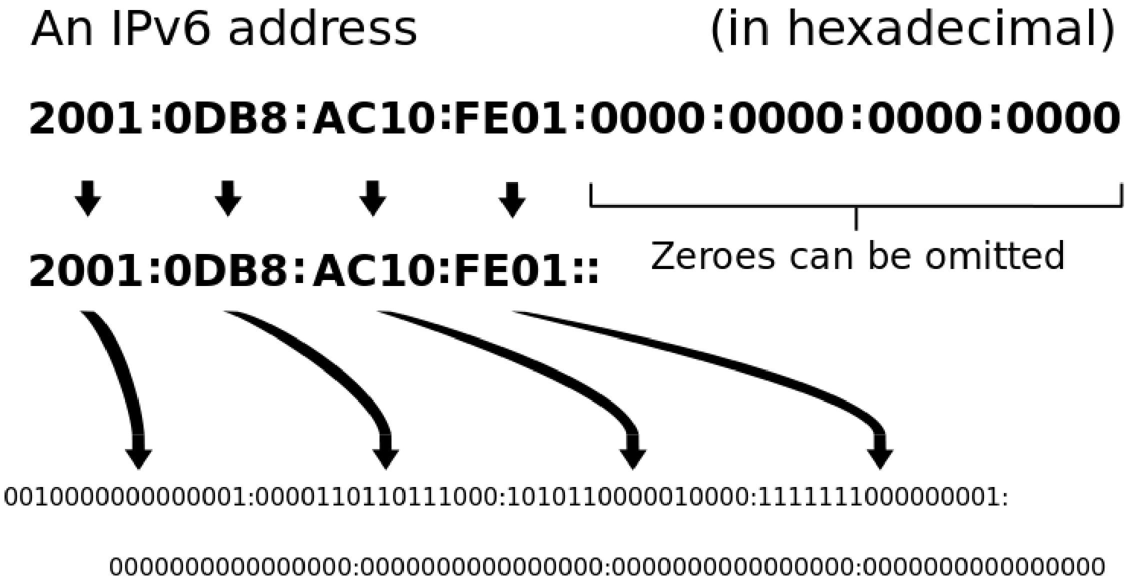


IPv6 Header (nh = 43)

Routing Header (nh = 6)

TCP Header

IPv6 Addressing



An IPv6 address (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

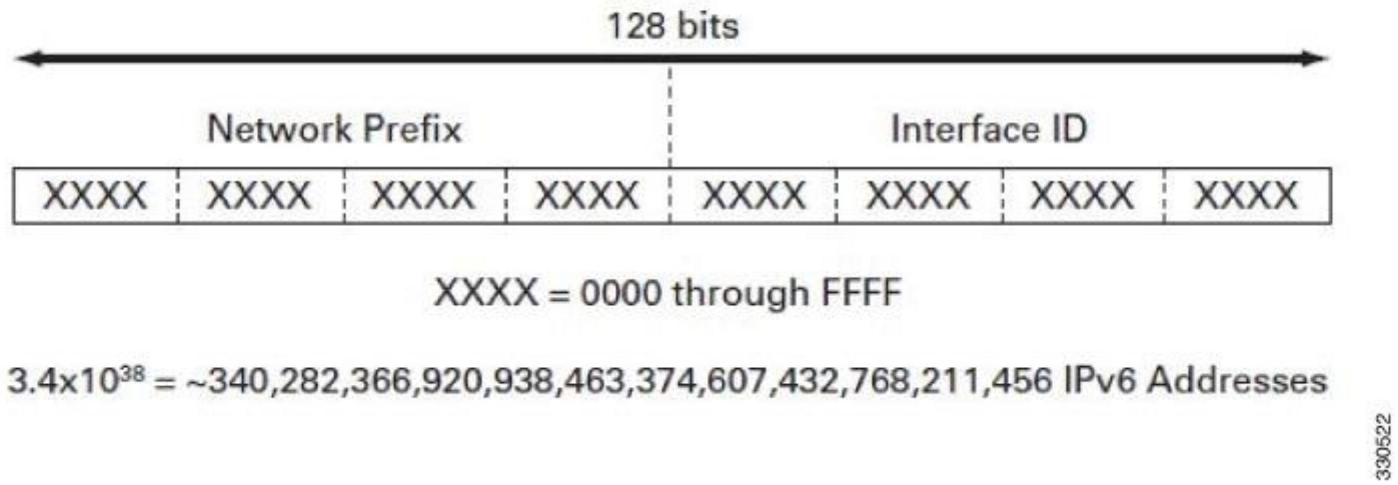
2001:0DB8:AC10:FE01::

Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

IPv6 Addressing



XXXX = 0000 through FFFF

$3.4 x 10^{38}$ = ~340,282,366,920,938,463,374,607,432,768,211,456 IPv6 Addresses

IPv6 Addressing

Commonly used address scopes:

Global

Site-Local

Link-Local

Multicast

Multicast Addresses

Address	Description	Available Scopes
ff0X::1	All Nodes	•Interface-Local •Link-Local
ff0X::2	All Routers	•Link-Local •Site-Local
ff0X::fb	mDNSv6	•All Scopes
ff02::1:3	Link-local Multicast Name Resolution	•Link-Local

ICMPv6

Enables the following:

Neighbor Discovery (NDP) and Secure Neighbor Discovery (SEND)

Multicast Listener Discovery (MLD)

Multicast Router Discovery (MRD)

ICMPv6

Bit offset	0–7	8–15	16–31
0	Type	Code	Checksum
32	Message body		

ICMPv6 Types

Value	Meaning
1	Destination Unreachable
128	Echo Request
129	Echo Reply
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
143	Multicast Listener Query (MLDv2)

Neighbor Discovery

Neighbor Discovery (ND) is the protocol used to discover other nodes on the same subnet

Uses ICMPv6

Enables the following:

- SLAAC
- Neighbor Solicitation and Advertisements
- Router Solicitation and Advertisements
- Duplicate Address Detection (DAD)

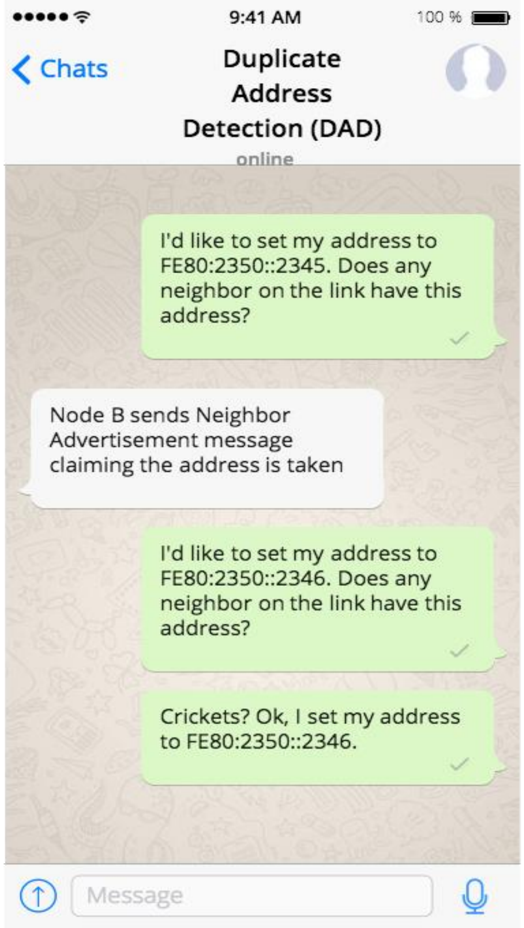
Neighbor Discovery

Router Solicitation – Clients use this type to locate routers on the local-link

Router Advertisement – Routers advertise their presence with advertisement messages

Neighbor Solicitation – Nodes use neighbor solicitation messages to determine layer 2 address addresses of other nodes and to verify if a node is still reachable

Neighbor Advertisement – Nodes use this message type to respond to solicitation messages



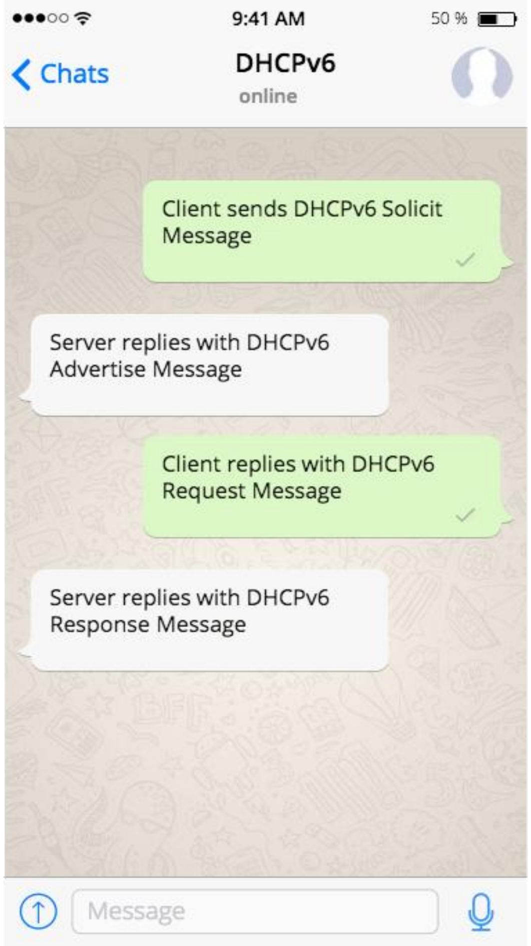
Duplicate Address Detection (DAD)

I'd like to set my address to FE80:2350::2345. Does any neighbor on the link have this address?

Node B sends Neighbor Advertisement message claiming the address is taken

I'd like to set my address to FE80:2350::2346. Does any neighbor on the link have this address?

Crickets? Ok, I set my address to FE80:2350::2346.



Client sends DHCPv6 Solicit Message ✓

Server replies with DHCPv6 Advertise Message

Client replies with DHCPv6 Request Message ✓

Server replies with DHCPv6 Response Message

Refresher Complete

THE INFORMATION PROVIDED IN THIS PRESENTATION IS INTENDED TO BE GENERAL IN NATURE AND IS NOT SPECIFIC GUIDANCE. RECOMMENDATIONS (INCLUDING POTENTIAL COST SAVINGS) ARE BASED UPON INTEL'S EXPERIENCE AND ARE ESTIMATES ONLY. INTEL DOES NOT GUARANTEE OR WARRANT OTHERS WILL OBTAIN SIMILAR RESULTS.