Internet Protocol version 6 (IPv6)

October 2021
Ben Patton, UNH-IOL

University of New Hampshire

Ben Patton

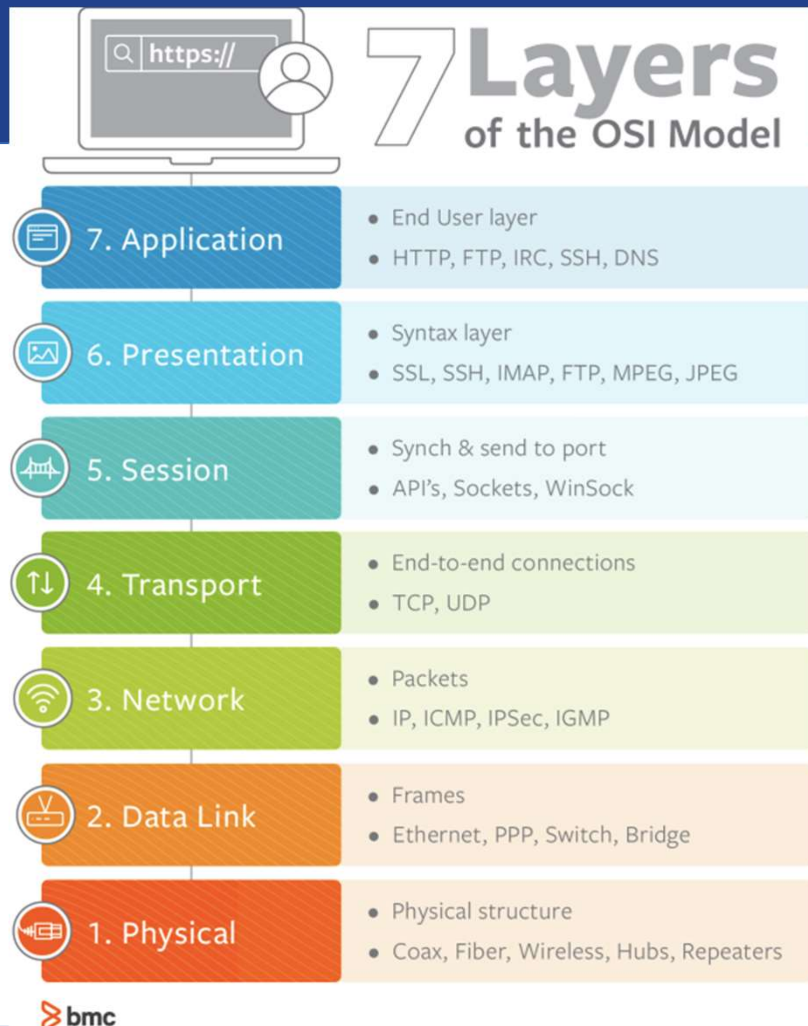
IPv6 Testing Team Scrum Master

UNH InterOperability Lab

10/26/2021

What is IPv6?

- Provides a method of identifying nodes on a network
  - IP Addresses
- Defines mechanisms for how nodes find each other and talk to each other
- Next version of the Internet Protocol
  - intended for widespread use, anyway: IPv5



<= IPv4 and IPv6 are at Layer 3

Why do we need IPv6?

- Primary motivation: increased address space
  - All IPv4 address ranges have been “allocated”
  - the world needs more addresses to meet demand now that we have so many internet-enabled devices

- IPv4 address space (theoretically) with 32 bits
  - 0.0.0.0 -> 255.255.255.255 = 2^{32} = 4,294,967,296
- IPv6 address space (theoretically) with 128 bits
  - 0::0 > ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff = 2^{128} = 3.4028237e+38 (something undecillion)

Why do we need IPv6?

- Improved protocol flexibility with extension headers
  - Changes to the IPv6 header that make formatting simple
- Addition of Stateless Address Autoconfiguration (SLAAC) as a method of assigning IP addresses

List of some relevant IPv6 RFCs

- RFC 2460 - Original IPv6 specification
- RFC 8200 - New and Revised IPv6 specification
- RFC 4443 - ICMPv6
- RFC 4861 - Neighbor Discovery for IPv6
- RFC 4862 - IPv6 Stateless Address Autoconfiguration

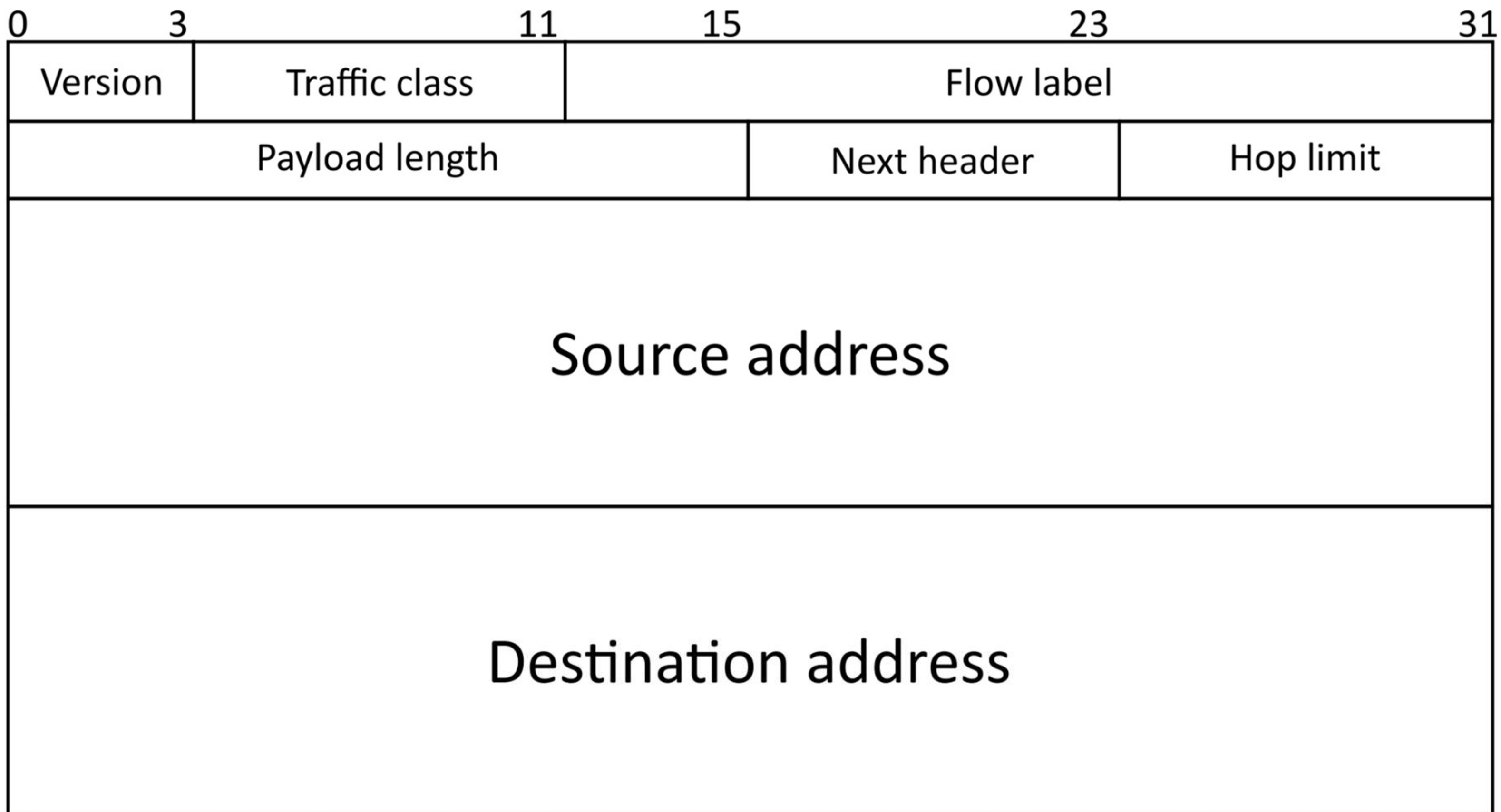
IPv4 and IPv6: What's the difference?

Some differences

	IPv4	IPv6
Number of possible addresses	2^32	2^128
Address notation	4 dot-separated decimal octets 132.177.234.18/24 192.168.1.14/24	8 groups of 16 bits, separated with colons (written in hexadecimal) 2606:3880:4100:1181:0250:10ff:fe10:1080/64 fe80::0250:10ff:fe10:1080/64
Address assignment	Auto-IP, DHCP, static	Stateless (SLAAC), DHCPv6, static
Neighbor Discovery	ARP	ICMPv6 messages
Header size	Varies	40 bytes (+ N * 8 bytes with extension headers)
Fragment processing	handled at each intermediate node	handled only at destinations

The IPv6 Header

October 2021
Ben Patton, UNH-IOL



IPv6 header fields

Version field (4 bits) - **Always** set to 6

Traffic Class (8 bits) - Used as a "priority" flag for nodes that prioritize processing/forwarding some packets over others

Flow Label (20 bits) - Can uniquely identify similar packets with similar data. Nodes *can* process packets with the same flow label more quickly/efficiently.

Payload Length (16 bits) - How many bytes are in this packet (includes IPv6 header and all upper-layer info)

Next Header (8 bits) - A number that denotes what kind of header follows the IPv6 header (could be an extension header, ICMP header, TCP/UDP, etc.)

Hop Limit (8 bits) - Denotes how many more routers this packet can go through before a router determines that it can't forward the packet to its destination. Similar to Time-To-Live.

IPv6 Extension Headers

- Additional headers beyond the base IPv6 header that include extra packet information
  - Only included as needed
  - Only processed by certain nodes depending on the extension header
- Inserted between the IPv6 header and any upper-layer protocol header (e.g. TCP, UDP, etc.)

```
+---------------+------------------------
|  IPv6 header  | TCP header + data
|               |
| Next Header = |
|      TCP      |
+---------------+------------------------

+---------------+----------------+------------------------
|  IPv6 header  | Routing header | TCP header + data
|               |                |
| Next Header = |  Next Header = |
|    Routing    |      TCP       |
+---------------+----------------+------------------------

+---------------+----------------+-----------------+-----------------
|  IPv6 header  | Routing header | Fragment header | fragment of TCP
|               |                |                 |  header + data
| Next Header = |  Next Header = |  Next Header =  |
|    Routing    |    Fragment    |       TCP       |
+---------------+----------------+-----------------+-----------------
```

List of Extension headers

- Fragment Header
  - Used when fragmenting large packets
- Routing Header
- Hop-by-Hop Options Header
- Destination Options Header
- Authentication (IPSec)
- Encapsulating Security Payload (IPSec)

October 2021
Ben Patton, UNH-IOL

Address Notation

IPv6 Addresses

- 128 bits written as 8 groups of 16 bits in hex
- Divided into 2 parts:
  - Prefix -> defines what network your on
  - Interface Identifier -> defines you uniquely on the link
  - Typically divided evenly, 64 bits for prefix, 64 bits for ID

2606:3880:4100:1181 -> **prefix** (given by router)
0200:10ff:fe10:1080 -> **interface ID** (created by node)

2606:3880:4100:1181:0200:10ff:fe10:1080/64 -> full address

Abbreviating IPv6 Addresses

Because who wants to write out all those hex characters?

Can remove leading zeros from each colon-separated group

- So… FE80:0000:0000:0000:0250:10FF:FE10:1080/64
- becomes FE80:0:0:0:250:10FF:FE10:1080/64

Can also use double-colon to remove groups of adjacent extra zeros, but double-colon can only appear once in the address

- So… FE80:0:0:0:250:10FF:FE10:1080/64
- becomes FE80::250:10FF:FE10:1080/64

Interface IDs

- Every IPv6 node has an "Interface ID"
  - The last 64 bits of an IPv6 address
  - Uniquely identifies the interface to others on-link
  - Traditionally based on the MAC address of the interface (called EUI-64 format)
    - Interface with a MAC of 52:57:3C:CC:AE:2C will create an interface ID of 5057:3CFF:FECC:AE2C
    - Flip a high order bit, then insert "ff:fe" in the middle to pad it out to 64 bits.
- A few security concerns about using your MAC to generate a globally unique IP address
  - Lead to creation of Stable-ID (RFC 7217) where ID used is also based on the prefix and a random number
  - Also Privacy and Temporary addressing, which use even more volatile IDs

Address Scope

- The prefix an IPv6 address has determines the scope of who receives it, more applicable to multicast
- Several different types of IPv6 address scope:
  - fe80::/64 -> link-local scope
  - ff00::/64 -> multicast scope
  - fc00::/8 or fd00::/8 -> unique local scope (deprecated)
  - fec0::/10 -> site local scope (also deprecated)
  - 2000::/64 to 3FFF::/64 -> global scope
- A node will use a link-local address to communicate with another node's link-local address
- A node will use a global address to communicate with another node's global address
- etc.

Address Scope

- There are some prefixes in IPv6 that are reserved for special cases, lots of them related to multicast

- ff**00**::/64 -> multicast prefix range
  - Different addresses in this range have special meanings
  - 00 highlighted in the prefix above determines scope
    - ff02::/64 is the on-link multicast prefix
    - ff04::/64 is the admin-local multicast prefix
    - etc.
  - the last part of the address in that range has a special meaning too
    - traffic sent to ff02::1 goes to all nodes on-link
    - traffic sent to ff05::3 goes to all site-local DNS servers

More info on special prefix scopes:

https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

page has a good explanation of different multicast scopes and special addresses within each scope.

Clarifying a few more terms..

Link-local vs. Global

- IPv6 nodes automatically create their own Link-local IPv6 address
- To talk to anything on a different network, they need a global address
  - Anything on a different network -> any destination that requires the node to send its packets to a router for forwarding.
  - Nodes create their own global addresses, but need information from a router to do so (global prefix in Router Advertisement messages)
- Global prefixes can be anything from 2000::/64 to 3FFF::/64

Unicast vs. Multicast vs. Anycast vs. Broadcast

Based on the intended destination of a given packet, there are different kinds of addresses to which a packet can be sent

Unicast -> Sent to a **single** destination. No other device receives the packet.

Multicast -> Sent to **potentially multiple** devices, destination is determined by address scope (See previous slide).

Anycast -> Sent to whichever destination is known to be closest/best for the sender.

Broadcast -> Sent to **everyone** on link. The term "broadcast" isn't used in the context of IPv6, mostly in IPv4. IPv6 Packets can be sent to everyone on link through use of a specific multicast address.

October 2021
Ben Patton, UNH-IOL

Neighbor Discovery, Router Discovery, and SLAAC

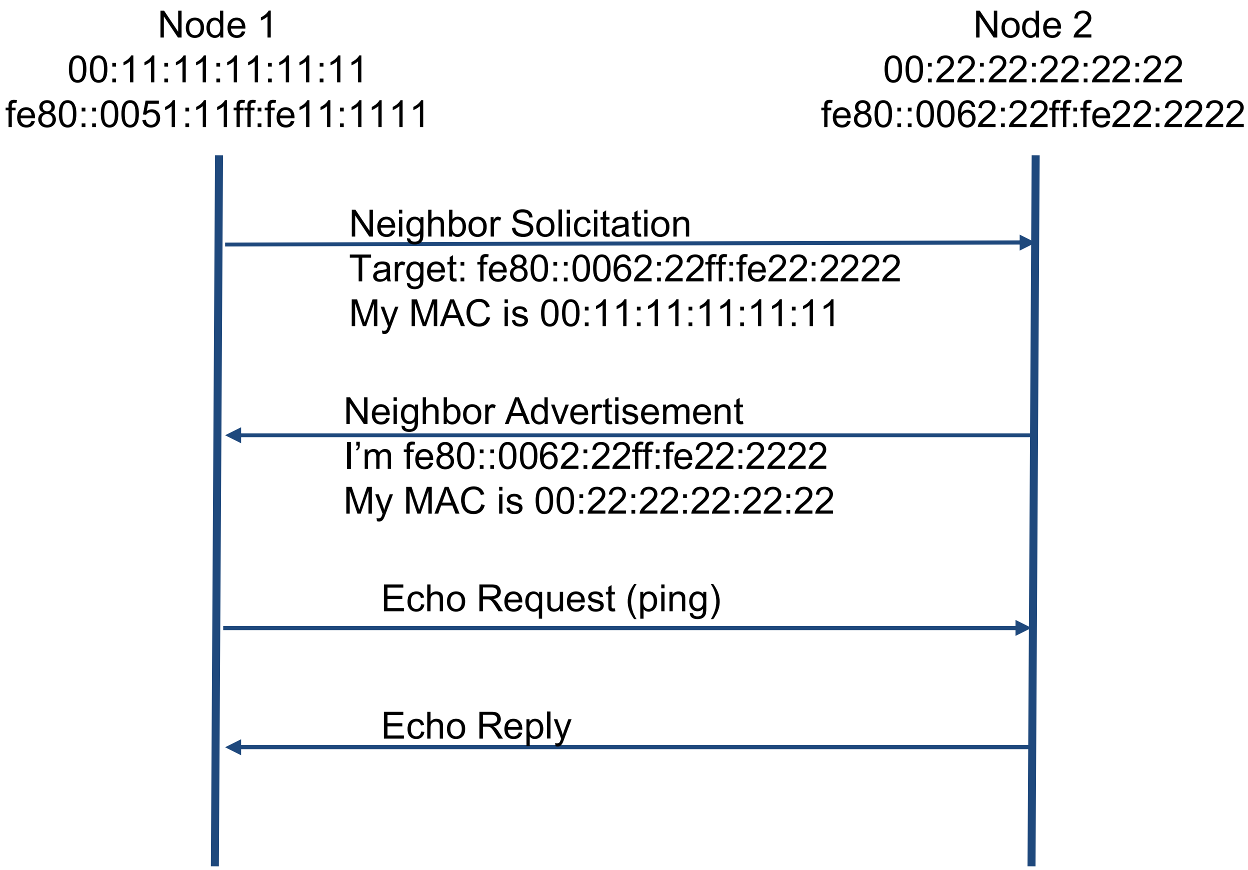
IPv6 ND

- All accomplished with ICMP packets
  - specifically Neighbor Advertisements and Neighbor Solicitations
  - ND mechanisms replace ARP from IPv4

- ICMPv6 Neighbor Solicitations
  - “Who has this IPv6 address on my network?”
- ICMPv6 Neighbor Advertisements
  - “The node with this IPv6 address is me, I have this MAC address”

Node1 wants to ping Node2

October 2021
Ben Patton, UNH-IOL



How do devices get new Addresses?

- SLAAC - Stateless Address Autoconfiguration
  - Also accomplished through ICMPv6 messages:
    - Router Solicitations
    - Router Advertisements
    - Neighbor Solicitations and Advertisements

- Routers can send special messages called Router Advertisements that tell everyone on the network what global address they can have

Duplicate Address Detection (DAD)

When a node wants to assign itself an address, it needs to make sure that address isn't already taken

Sends a special Neighbor Solicitation to check

- Source all zeros ("0::0" or "::" AKA "unspecified address")
- Destination is special multicast address (solicited-nodes multicast address)

If it detects that someone else is using that address, it can either try a different one or disable that interface

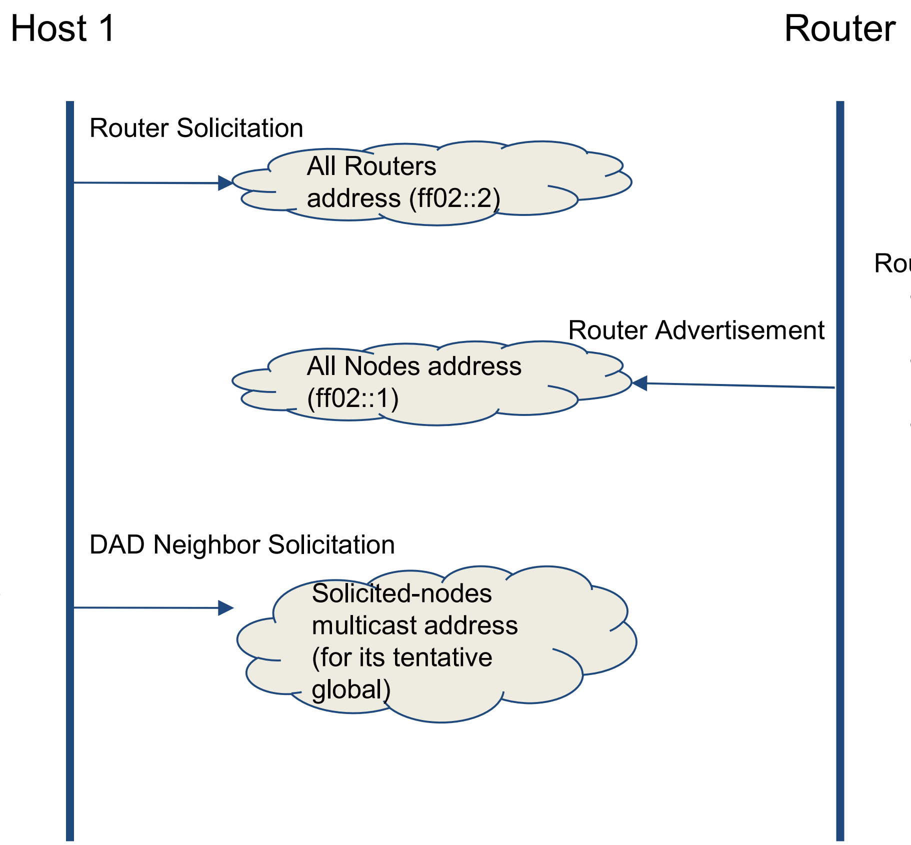
Router Discovery & SLAAC

October 2021
Ben Patton, UNH-IOL

Host 1 sees the Router Advertisement, uses the included prefix to configure its own Global IPv6 address.

2001:2:0:1000::/64 -> prefix from router
0250:10ff:fe10:1080 -> interface ID generated by host

puts them together to create a full IPv6 address, sends DAD NS to ensure it's unique.



Router advertisement contains:

- Global IPv6 prefix (e.g. 2001:2:0:1000::/64)
- How long the device sending the RA can be used as a router (lifetime)
- Some additional ND information

Quick Demo

With a live wireshark capture and some linux nodes, if time permits

Where is IPv6 deployment at today?

IPv6 World launch:
https://www.worldipv6launch.org/measurements/

Google IPv6 adoption maps:
https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption

6lab from Cisco:
https://6lab.cisco.com/stats/

Why are we not only using IPv6 now?

Because changing the world takes time

- All previous infrastructure and knowledge about IPv4 doesn't just go away, some systems and organizations rely on it
- NAT used as a band-aid to slow consumption of global IPv4 addresses
- Support for IPv6 isn't *completely* universal yet
- Mechanisms exist for IPv6 and IPv4 to work together (6to4, Tunneling mechanisms, etc.)

Thanks!

Questions, if you have them?