IPv6 in Wireshark

Troubleshooting IPv6 with Wireshark

Tuesday June 14, 2016

jeff.carrell@teachmeipv6.com
Twitter: @JeffCarrell_v6

Jeffrey L Carrell
Network Consultant, IPv6 SME/Trainer – Network Conversions

IPv6 – a bit more than basics
Wireshark basics
Wireshark color rules, display filters, columns, configuration profiles, and packet annotation
IPv6 in Wireshark: hands-on labs
IPv6: Trivia

• In modern day operating systems, is IPv6 an enabled protocol?  **YES!**

• Generally, will an IPv6 enabled interface have more than one IPv6 address assigned to it?  **YES!**

IPv6: Trivia

• How many IPv6 GUA addresses can a network interface have that are in the same network?  **Up to 4!**

• How many IPv6 GUA addresses can a network interface have that are in different networks?  **Almost infinite!**

• Can the IPv6 Link-Local address be the same address for all network interfaces in a host?  **YES!**
IPv6: Trivia

• How does an IPv6 enabled host derive its default gateway?  **Via the RA!**

• Does DHCPv6 have a configurable option to provide an IPv6 default gateway?  **NO!**

• Does an IPv6 host use its LL or GUA address to communicate to its default gateway?  **LL!**

IPv6: Trivia

• If an IPv6 enabled host has autoconfigured privacy extension addresses and a statically assigned address, which one gets used for off-net communications?  **Temporary!**

• If attempting to communicate on-net using your GUA to another IPv6 host, will the communication be successful if the v6 router is not on-net?  **NO!**
IPv6 in Wireshark

IPv6 – a bit more than basics

• Quick IPv6 history
• IPv6 Address basics
• IPv6 Address Autoconfiguration
• IPv6 in applications

IPv6 Brief History

• Fall 1992 – IPv4 addresses will run out someday
• Oct 1993 – DHCP – RFC 1531 – easier IPv4 address management
• Dec 1993 – IPng – RFC 1550 – basic specification for next version IP
• May 1994 – NAT – RFC 1631 – temporary solution before IPng available
• Dec 1995 – RFC 1883 – Basic specifications of IPv6
• Feb 1996 – RFC 1918 – Private IPv4 addresses
• Dec 1998 – RFC 2460 – Full IPv6 defined
• May 2005 – RFC 3927 – APIPA (IPv4)
Comparing IPv4 & IPv6 Addresses

• IPv4 addresses $2^{32} = 4,294,967,296$
• IPv6 addresses $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$
  • which is 340 undecillion
    • 340 trillion trillion trillion
  • 79,228,162,514,264,337,593,543,950,336 times more v6 addresses than v4
• If IP addresses weighed one gram each:
  • IPv4 = half the Empire State Building
  • IPv6 = 56 billion earths

What is an IPv6 Address?

• IPv6 addresses are very different than IPv4 addresses in the size, numbering system, and delimiter between the numbers
  • 128bit -vs- 32bit
  • colon-hexadecimal -vs- dotted-decimal
  • colon and double colon -vs- period (or “dot” for the real geeks)
• Valid IPv6 addresses are comprised of hexadecimal numbers (0-9 & a-f), with colons separating groups of four numbers, with a total of eight groups
  (each group is known as “quibble” or “hextet”)
  • 2001:0db8:1010:61ab:f005:ba11:00da:11a5
IPv6 default for subnet

- Based on the default definition an IPv6 address is logically divided into two parts: a 64-bit network prefix and a 64-bit interface identifier (IID)
- Therefore, the default subnet size is /64
- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64

A single /64 network yields **18 billion-billion** possible addresses

IPv6 shorthand notation

Option 1 **2001::a52:0:0:0:3d16**

- Consecutive Zeros
- Leading Zeros

Option 2 **2001:0000:0000:0a52:0000:0000:0000:3d16**

- Leading Zeros
- Consecutive Zeros
Incorrect shorthand notation

Address types

<table>
<thead>
<tr>
<th>Address Type</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- One-to-one communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>- One-to-many communication local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- One-to-many communication local/remote</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anycast</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>- One-to-many communication nearest</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Address scopes

<table>
<thead>
<tr>
<th>Address Scope</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local</td>
<td>Yes (is temp, APIPA)</td>
<td>Yes</td>
</tr>
<tr>
<td>- Not routable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Unicast</td>
<td>Aka public</td>
<td>Yes</td>
</tr>
<tr>
<td>- Routable to Internet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unique Local</td>
<td>RFC 1918 Aka private</td>
<td>RFC 4193</td>
</tr>
<tr>
<td>- Routable only within domain</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IPv4/IPv6 special addresses

<table>
<thead>
<tr>
<th>Address Type</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Route</td>
<td>0.0.0.0/0</td>
<td>::/0</td>
</tr>
<tr>
<td>Unspecified</td>
<td>0.0.0.0/32</td>
<td>::/128</td>
</tr>
<tr>
<td>Loopback</td>
<td>127.0.0.1/8</td>
<td>::/128</td>
</tr>
<tr>
<td>Multicast</td>
<td>224.0.0.0/4</td>
<td>ff00::/8</td>
</tr>
<tr>
<td>Link-Local</td>
<td>169.254.0.0/16</td>
<td>fe80::/10</td>
</tr>
<tr>
<td>Global Unicast</td>
<td>All others</td>
<td>2000::/3</td>
</tr>
<tr>
<td>Unique Local</td>
<td>10.0.0.0/8</td>
<td>fc00::/7</td>
</tr>
<tr>
<td></td>
<td>172.16.0.0/12</td>
<td>(assigned from fd00::/8)</td>
</tr>
<tr>
<td>Documentation</td>
<td>192.0.2.0/24</td>
<td>2001:db8::/32</td>
</tr>
<tr>
<td></td>
<td>198.51.100.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>203.0.113.0/24</td>
<td></td>
</tr>
</tbody>
</table>
### IPv6 well known multicast addresses

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff01::1</td>
<td>All nodes address</td>
<td>Interface-local</td>
</tr>
<tr>
<td>ff02::1</td>
<td>All nodes address</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff01::2</td>
<td>All routers address</td>
<td>Interface-local</td>
</tr>
<tr>
<td>ff02::2</td>
<td>All routers address</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff05::2</td>
<td>All routers address</td>
<td>Site-local</td>
</tr>
<tr>
<td>ff02::4</td>
<td>DVMRP routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::5</td>
<td>OSPF routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::6</td>
<td>OSPF designated routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::9</td>
<td>RIPng routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::a</td>
<td>EIGRPv6 routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::d</td>
<td>All PIM routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::16</td>
<td>ALL MLDv2 routers</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::1:2</td>
<td>DHCPv6 servers/agents</td>
<td>Link-local</td>
</tr>
<tr>
<td>ff02::1:3</td>
<td>DHCPv6 servers/agents</td>
<td>Site-local</td>
</tr>
<tr>
<td>ff02::1:ffxx:xxxx</td>
<td>Solicited node address</td>
<td>Link-local</td>
</tr>
</tbody>
</table>

---

### Interface ID from MAC address

![Diagram of how to calculate an Interface ID from a MAC address.](image)

- **Company ID**
- **Manufacturer Data**

**IEEE 48-Bit MAC Address**

00 19 71 64 3F 00

- **0xFFFE inserted**
- **Expand to EUI-64 (IEEE Extended Unique ID)**

02 19 71 FF FE 64 3F 00

- **Invert the Local/Global Bit**
- **Modified EUI-64 Interface ID**

0219:71ff:fe64:3f00
Interface ID from Random Number

- RFC4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- Initial IID is derived based on mathematical computation to create a “random 64bit number” and appended to prefix to create a GUA
- An additional but different 64bit number is computed, appended to prefix, and tagged “temporary” for a 2nd GUA
- Temporary GUA should be re-computed on a frequent basis
- Temporary GUA is used as primary address for communications, as it is considered “more secure”

Lifetime states of an IPv6 address

- Tentative – address is in process of verification for uniqueness and is not yet available for regular communications
- Valid – address is valid for use in communication based on Preferred and Deprecated status
- Preferred – address is usable for all communications
- Deprecated – address can still be used for existing sessions, but not for new sessions
- Invalid – an address is no longer available for sending or receiving
## Comparing IPv4 & IPv6 Neighbor Discovery Protocols

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Request</td>
<td>Neighbor Solicitation</td>
</tr>
<tr>
<td>ARP Reply</td>
<td>Neighbor Advertisement</td>
</tr>
<tr>
<td>Router Solicitation</td>
<td>Router Solicitation</td>
</tr>
<tr>
<td>Router Advertisement</td>
<td>Router Advertisement</td>
</tr>
<tr>
<td>Gratuitous ARP</td>
<td>Duplicate Address Detection</td>
</tr>
<tr>
<td>ARP Cache</td>
<td>Neighbor Cache</td>
</tr>
</tbody>
</table>

## IPv6 Neighbor Discovery Protocol

- Neighbor Discovery Protocol (NDP) is defined in RFC 4861
- NDP provides the following basic IPv6 functions per node
  - Discover what link they are one
  - Learn link prefix addresses
  - Discover the on-link router
  - Discover on-link neighbors
  - Keep track of active neighbors
**NDP ICMPv6 message types**

- ICMPv6 type 133 - Router Solicitation (RS)
- ICMPv6 type 134 - Router Advertisement (RA)
- ICMPv6 type 135 - Neighbor Solicitation (NS)
- ICMPv6 type 136 - Neighbor Advertisement (NA)

---

**IPv6 autoconfiguration options**

<table>
<thead>
<tr>
<th>Address Autoconfiguration Method</th>
<th>ICMPv6 RA (Type 134)</th>
<th>ICMPv6 RA (Type 134) Prefix Info</th>
<th>Prefix Derived from</th>
<th>Interface ID Derived from</th>
<th>Other Configuration Options</th>
<th># of IPv6 Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local (always configured)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Internal (fe80::)</td>
<td>Manual</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>RA</td>
<td>Manual</td>
</tr>
<tr>
<td>Stateful (DHCPv6)</td>
<td>On</td>
<td>N/R</td>
<td>Off</td>
<td>On</td>
<td>DHCPv6</td>
<td>2 (LL, DHCPv6)</td>
</tr>
<tr>
<td>Stateless DHCPv6</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>RA</td>
<td>2 (LL, DHCPv6)</td>
</tr>
<tr>
<td>Combination Stateless &amp; DHCPv6</td>
<td>On</td>
<td>N/R</td>
<td>On</td>
<td>On</td>
<td>RA and DHCPv6</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
</tbody>
</table>

Copyright © 2016 Jeffrey L. Carrell
IPv6 in Wireshark

IPv6 Stateful (DHCPv6) process

• DHCPv6Solicit = DHCPDiscover (IPv4)
• DHCPv6Advertise = DHCPOffer (IPv4)
• DHCPv6Request = DHCPRequest (IPv4)
• DHCPv6Reply = DHCPAck (IPv4)

Wireshark

• Wireshark basics
• Wireshark
  • color rules
  • display filters
  • columns
  • configuration profiles
  • packet annotation
• Wireshark labs!!!
Wireshark main view

1. Title bar — trace file name or capture device name
2. Main menu — standard menu
3. Main toolbar — quick access
4. Display filter area — reduce the amount of traffic you see
5. Packet List pane — summary of each frame
6. Packet Details pane — dissected frames
7. Packet Bytes pane — hex and ASCII details
8. Status Bar — access to the Expert, annotations, file location, packet counts, and profiles

Jeff's IPv6 Wireshark
Coloring rules

- Colors help you focus on specific address, protocols, events, and possibly find errors quickly.

Color rule processing order

- Color rules read like a router ACL or firewall rule
  - First color rule that matches wins
Using Wireshark to view IPv6 pkts

- IPv6 display filter families
  - ipv6
  - icmpv6
  - dhcpv6
- IPv6 related display filters:
Display filters – option 1

- The Filter bar will change colors as you type to signify correct syntax for the filter
  - Green – syntax is correct
  - Red – syntax is incorrect
  - Yellow – syntax is suspect
- The Filter dropdown will show last 10 filters used
- You can save Filter definitions for frequent use

Display filters – option 2

- In the Packet Details view, right-click on a specific field to build a filter
Columns

- Right-click column headings to rename, align, etc
- In the Packet Details view, right-click on a specific field to Apply as Column
Configuration profiles

- What they are
- Why/how you use them
- What they contain
- How to share

Packet annotation

- Right click packet, select Packet Comment
Packet annotation

Wireshark demo #1 – watch me

Time for a Demo ☺☺ ☺☺
Resources

IPv6 in Wireshark v1.5 • Copyright © 2016 Jeffrey L. Carrell
SharkFest '16 • Computer History Museum • June 13-16, 2016

Resources

IPv6 in Wireshark v1.5 • Copyright © 2016 Jeffrey L. Carrell
SharkFest '16 • Computer History Museum • June 13-16, 2016
Resources

Thank You for Attending!

jeff.carrell@teachmeipv6.com

Twitter: @JeffCarrell_v6