SharkFest '16

Troubleshooting IPv6 with Wireshark

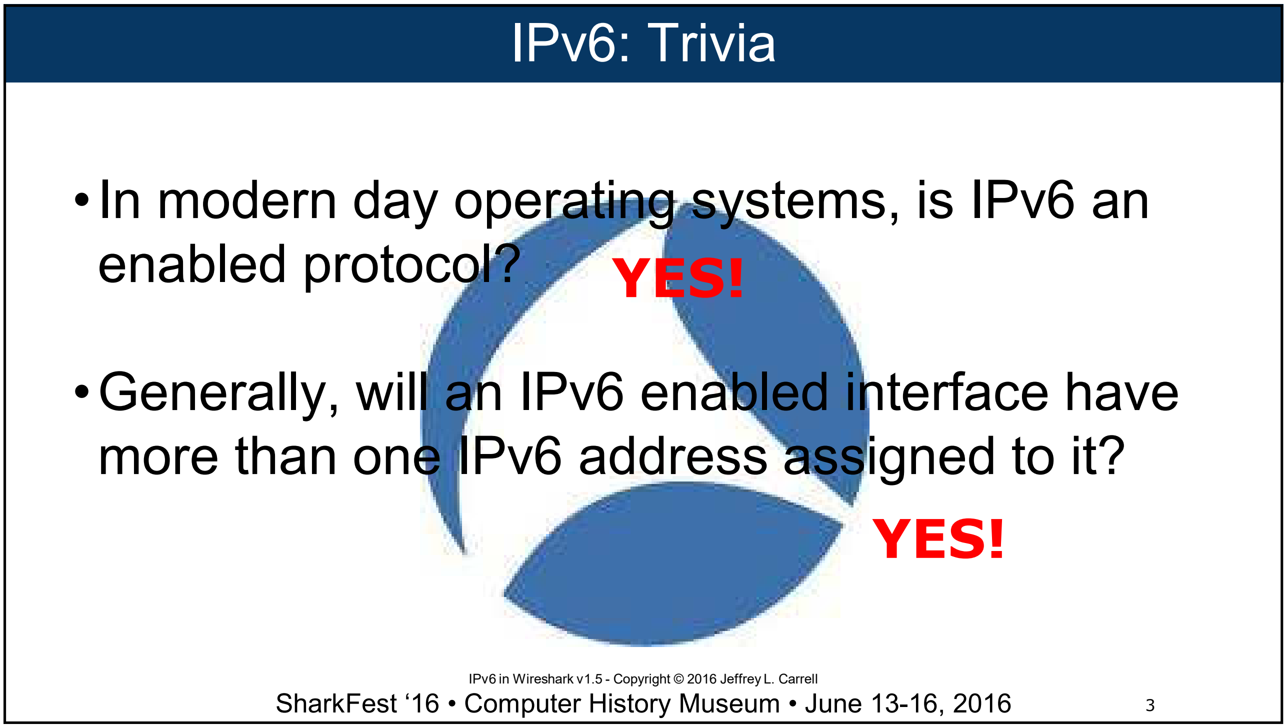
Tuesday June 14, 2016

jeff.carrell@teachmeipv6.com
Twitter: @JeffCarrell_v6

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

IPv6 in Wireshark

- 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

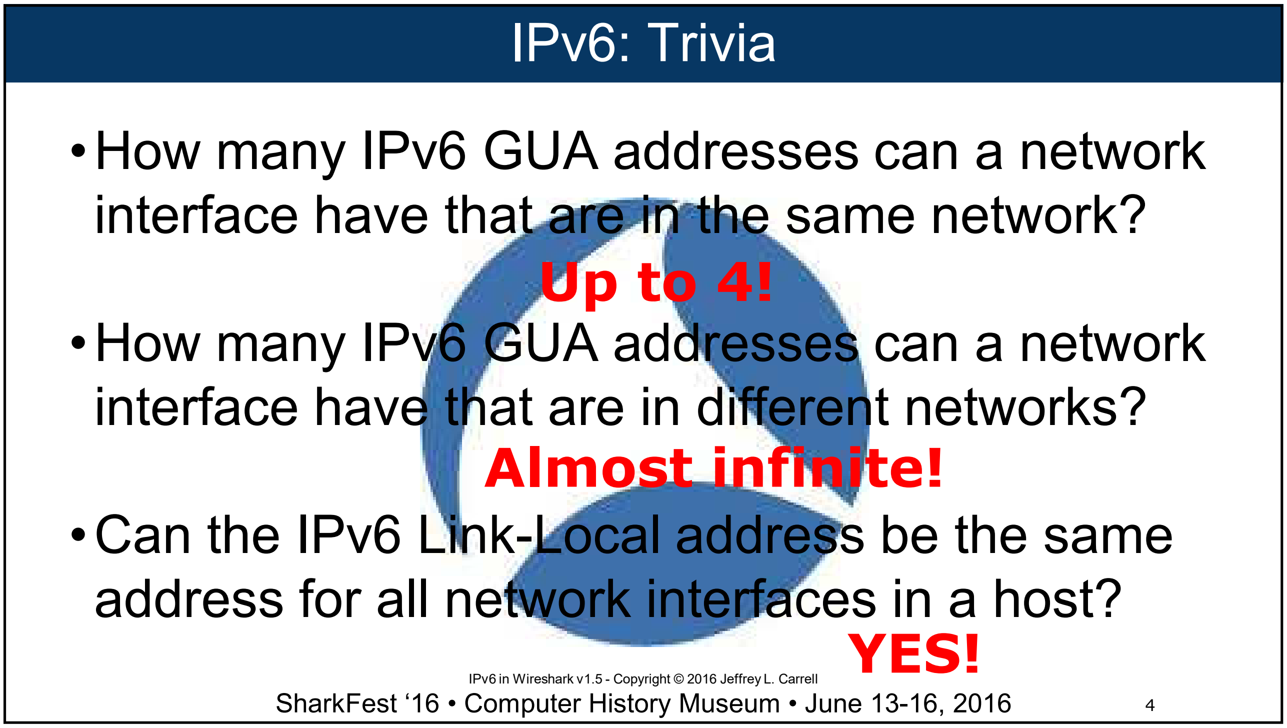


IPv6: Trivia

- 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 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 3

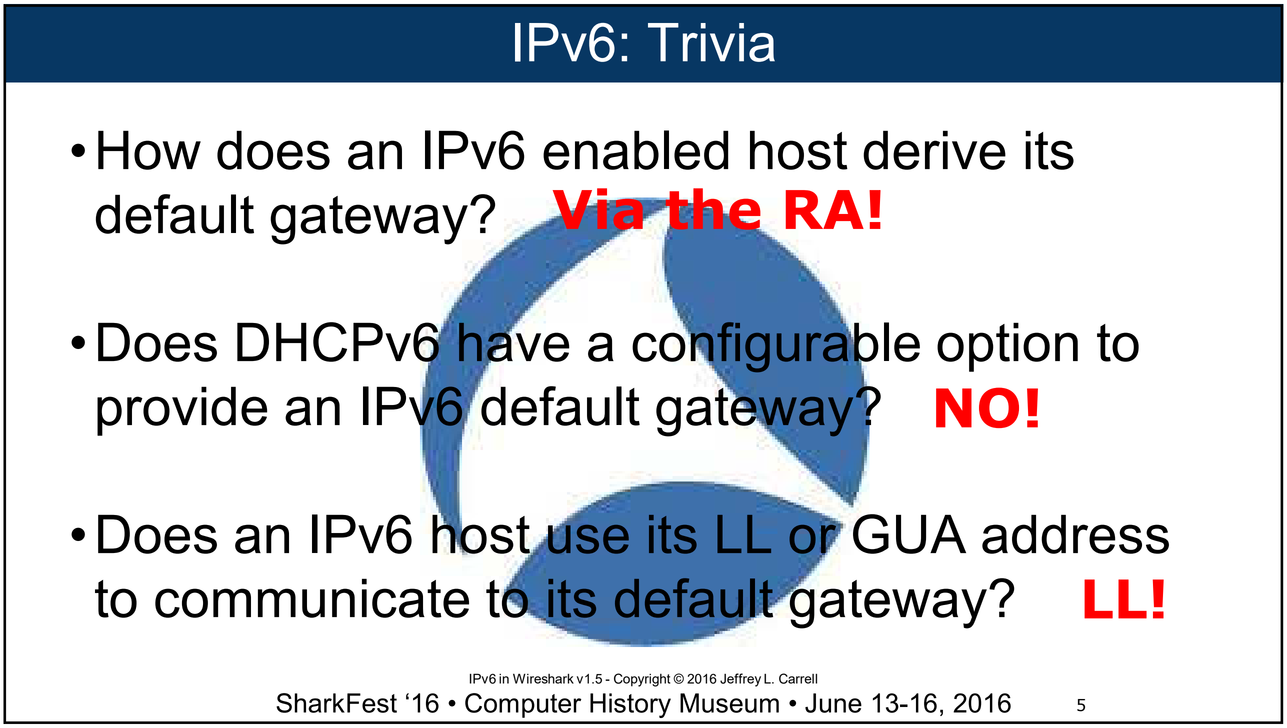


IPv6: Trivia

- 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!**

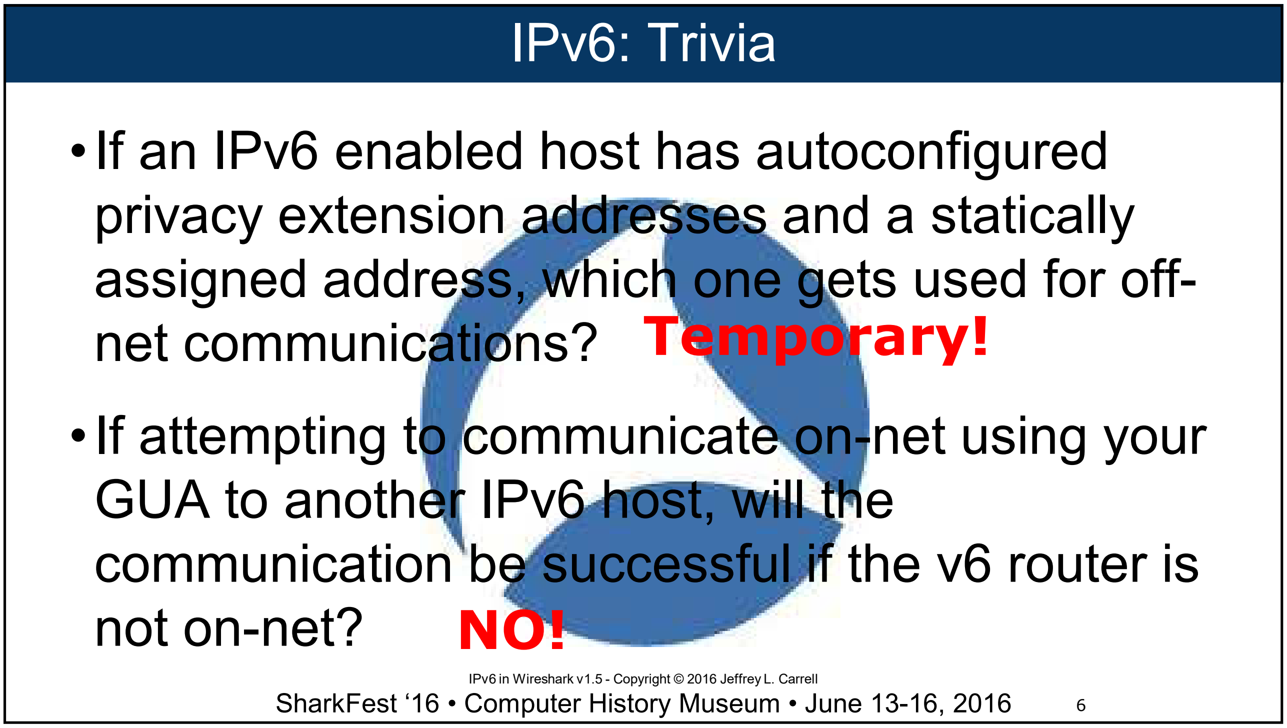
IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 4



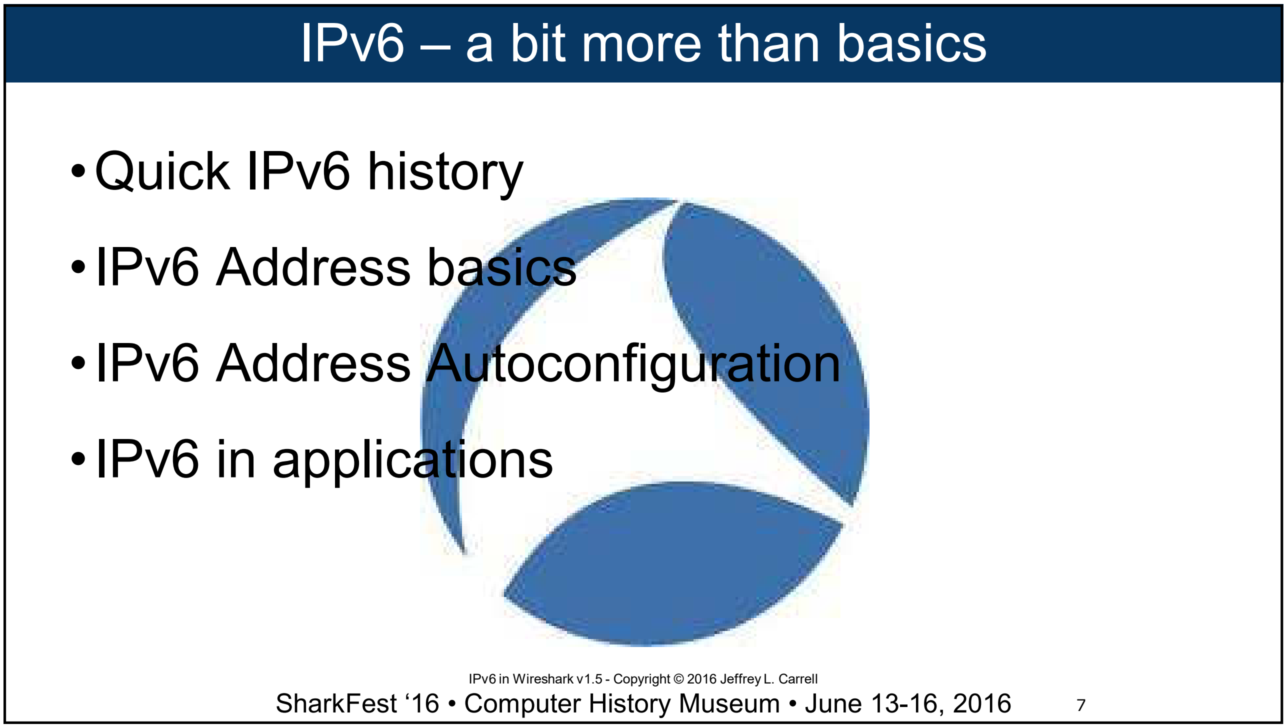
IPv6: Trivia

- 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!**



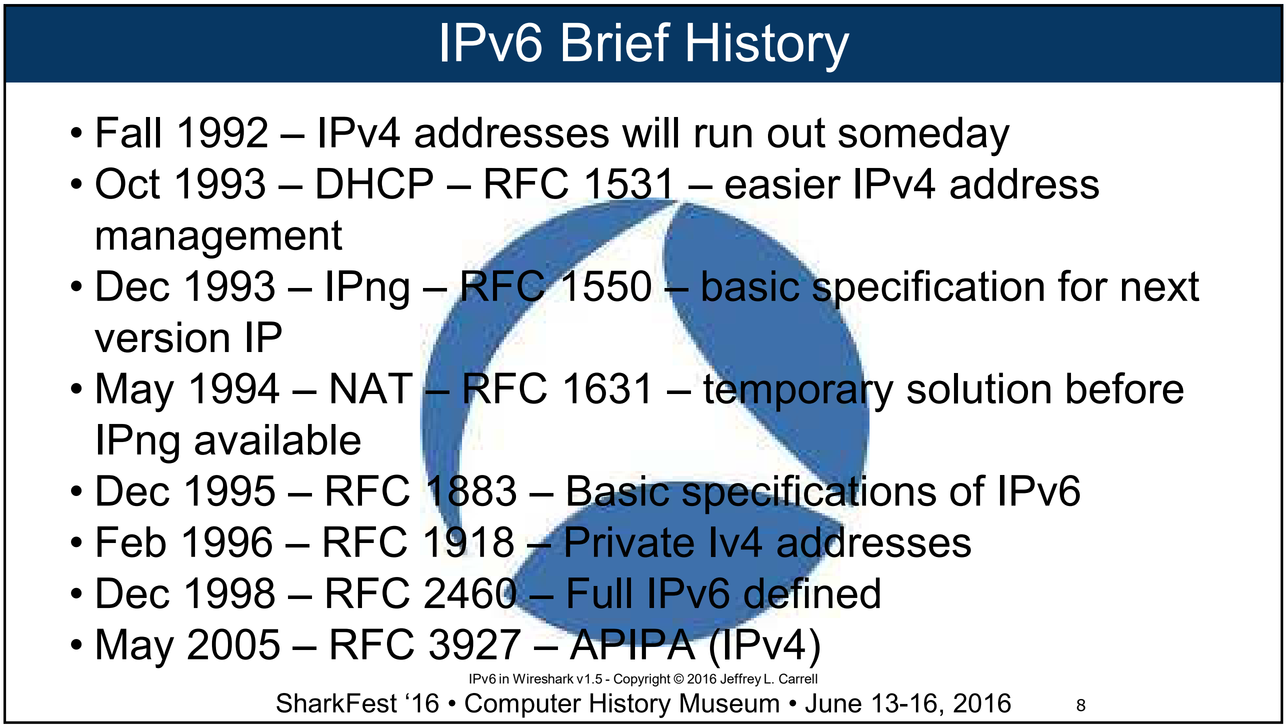
IPv6: Trivia

- 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!**



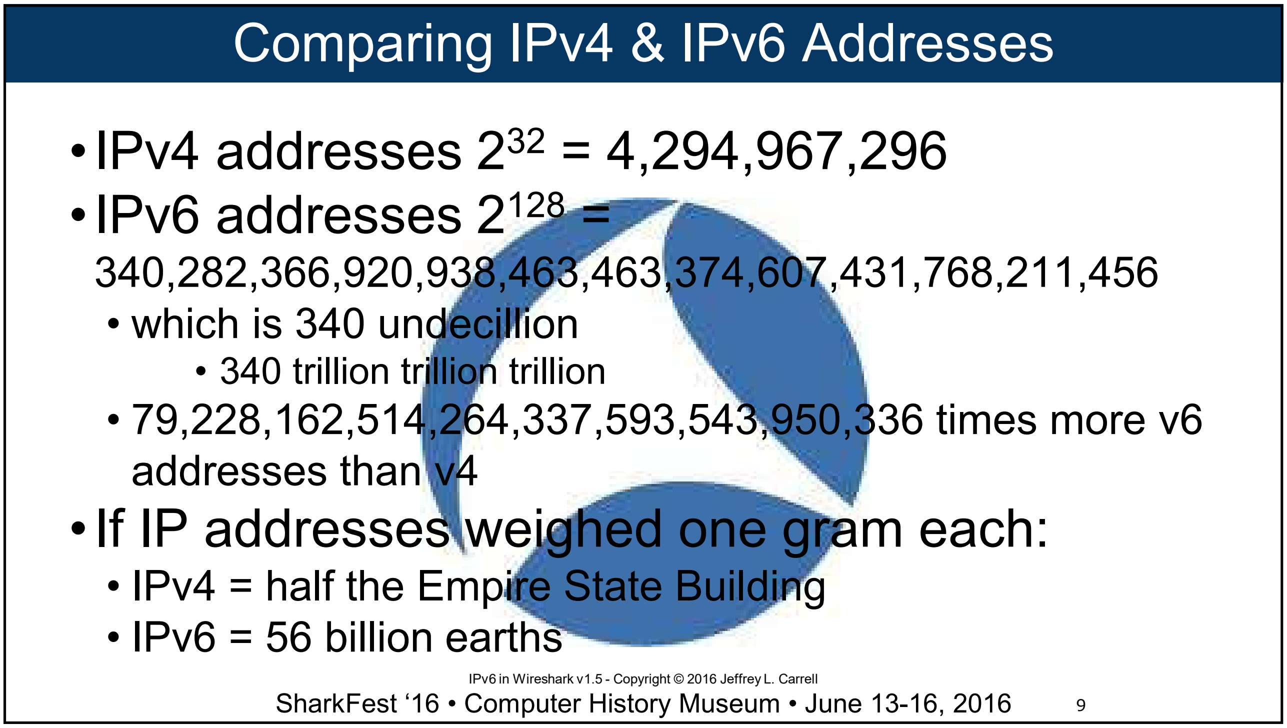
IPv6 – a bit more than basics

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



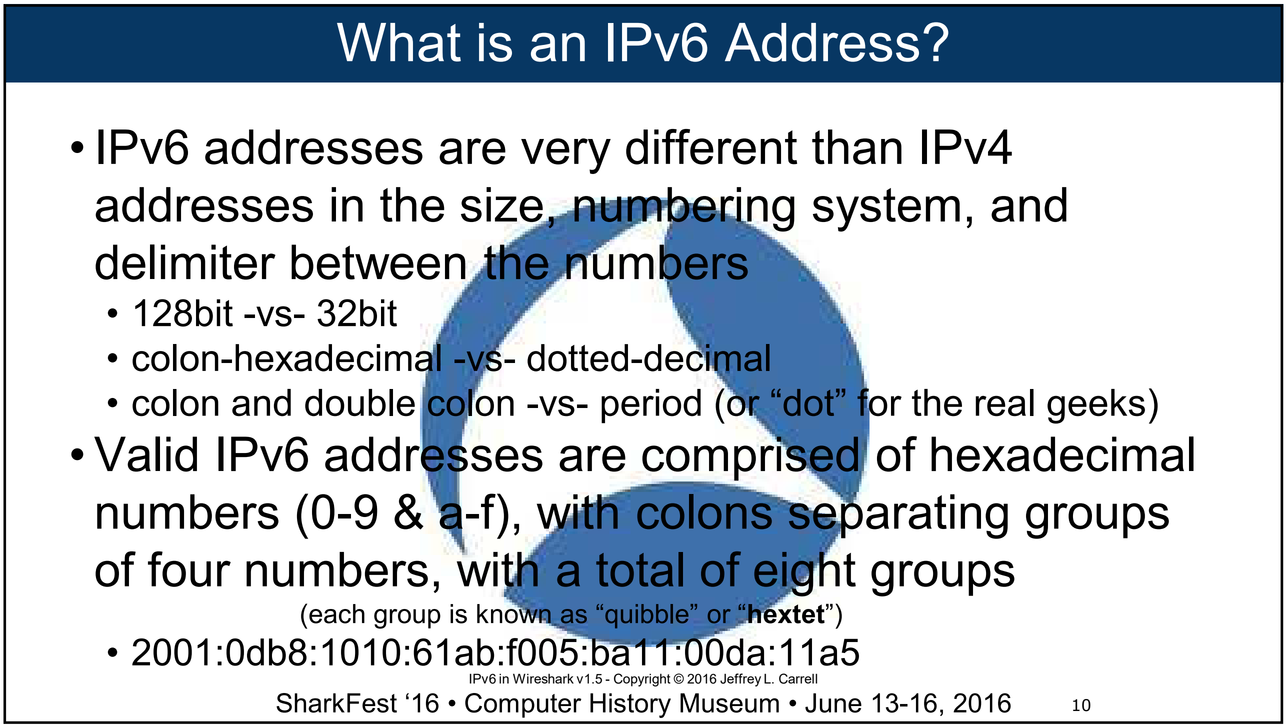
IPv6 Brief History

- 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 Iv4 addresses
- Dec 1998 – RFC 2460 – Full IPv6 defined
- May 2005 – RFC 3927 – APIPA (IPv4)



Comparing IPv4 & IPv6 Addresses

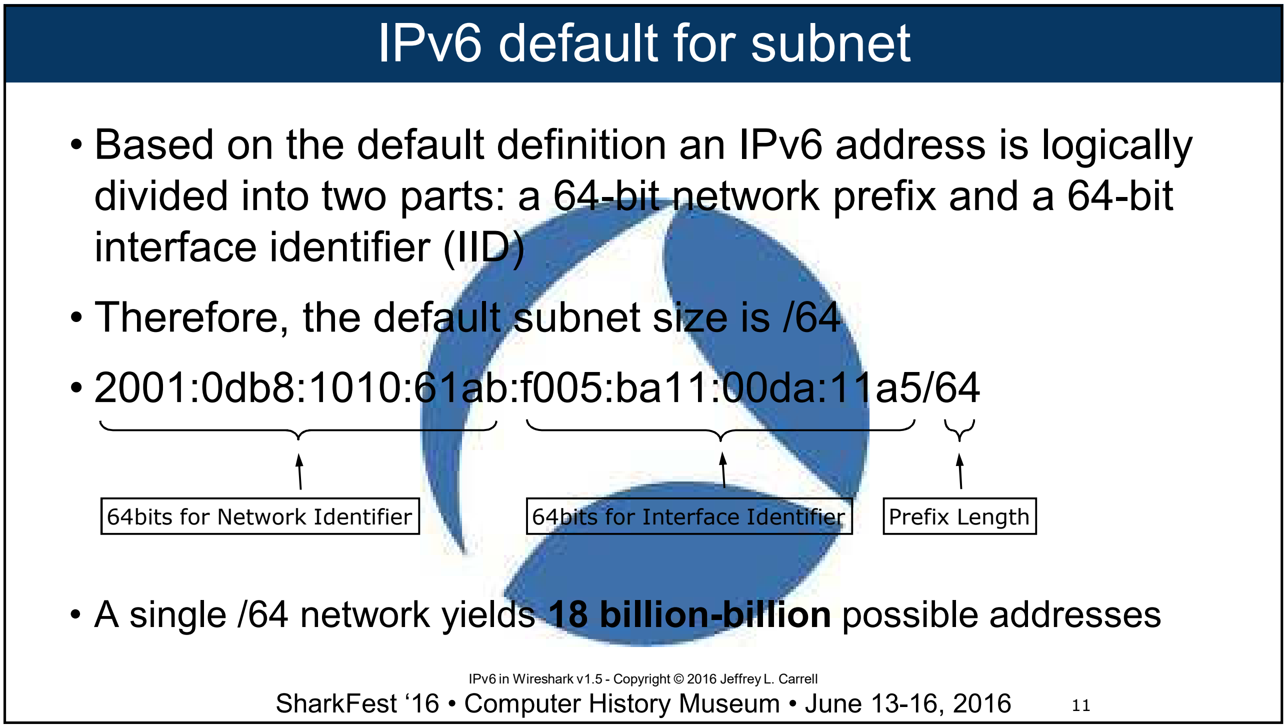
- IPv4 addresses 2^{32} = 4,294,967,296
- IPv6 addresses 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456
  - which is 340 undecillion
    - 340 trillion trillion trillion
  - 79,228,162,514,264,337,593,543,950,336 times more v6 addresses than v4
- If IP addresses weighed one gram each: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

64bits for Network Identifier

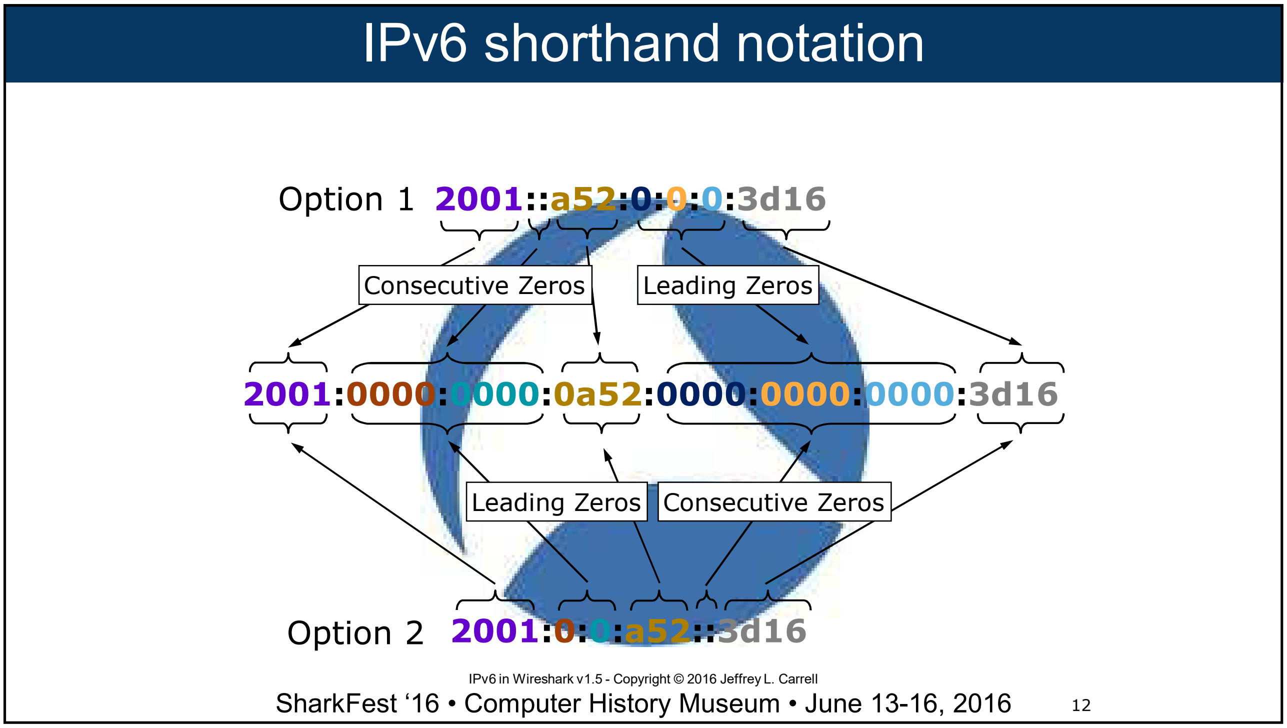
64bits for Interface Identifier

Prefix Length

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

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 11



IPv6 shorthand notation

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

Consecutive Zeros

Leading Zeros

2001:0000:0000:0a52:0000:0000:0000:3d16

Leading Zeros

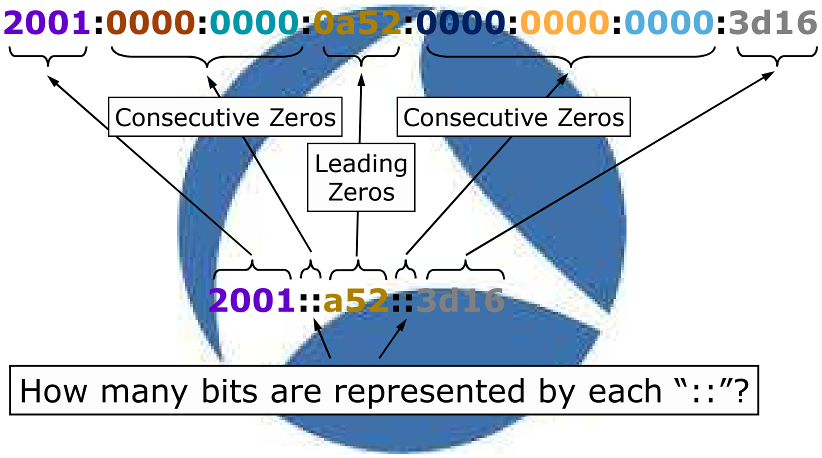
Consecutive Zeros

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

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 12

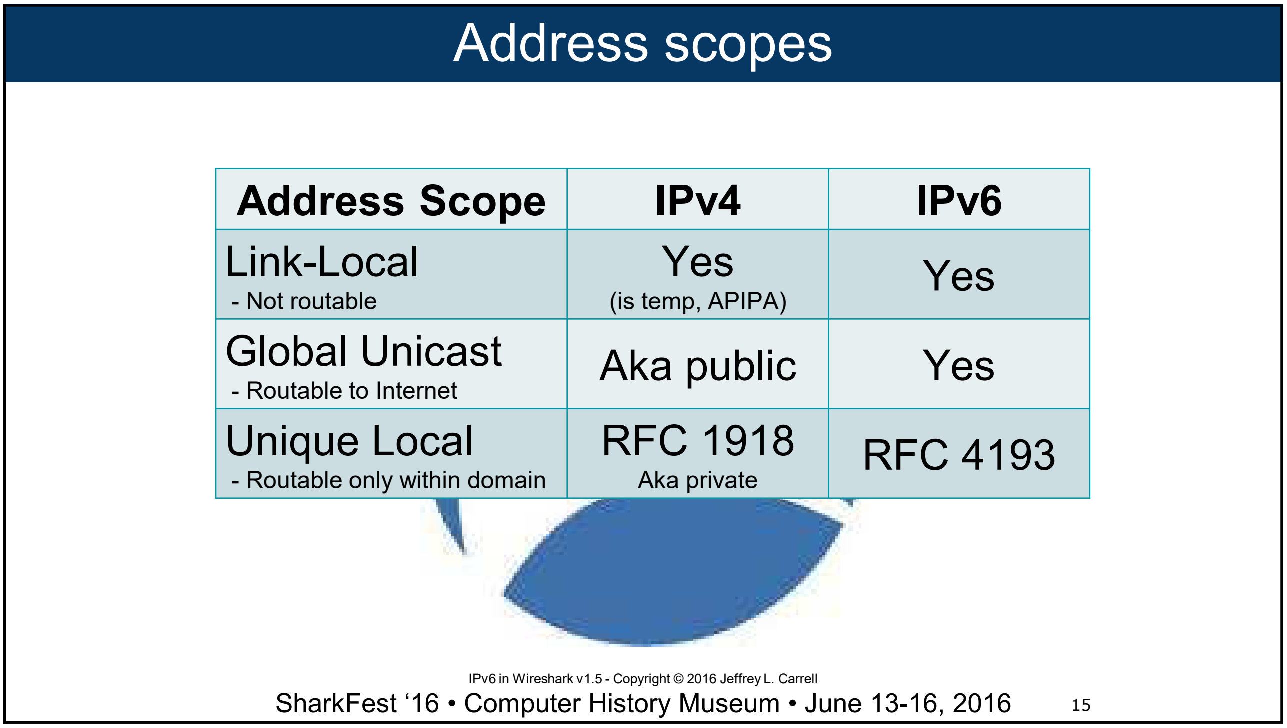
Incorrect shorthand notation



How many bits are represented by each "::"?

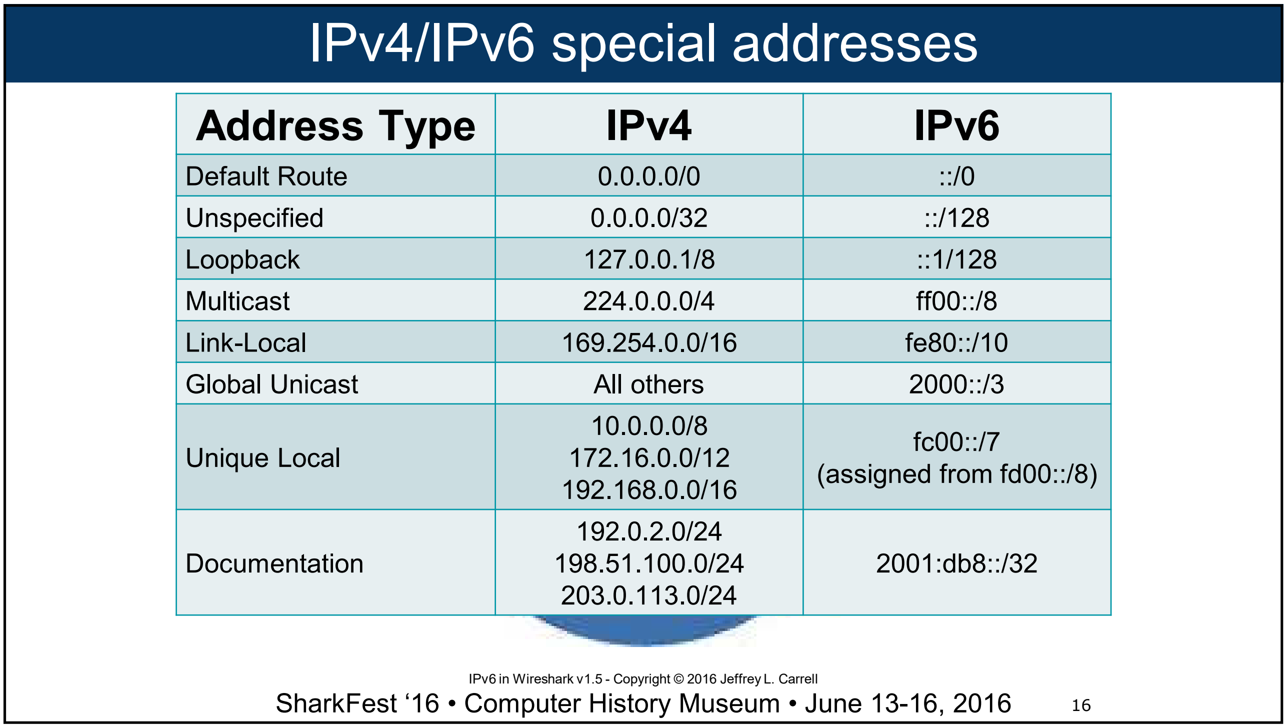
Address types

Address Type	IPv4	IPv6
Unicast - One-to-one communication	Yes	Yes
Broadcast - One-to-many communication local	Yes	**No**
Multicast - One-to-many communication local/remote	Yes	Yes
Anycast - One-to-many communication nearest	Yes	Yes



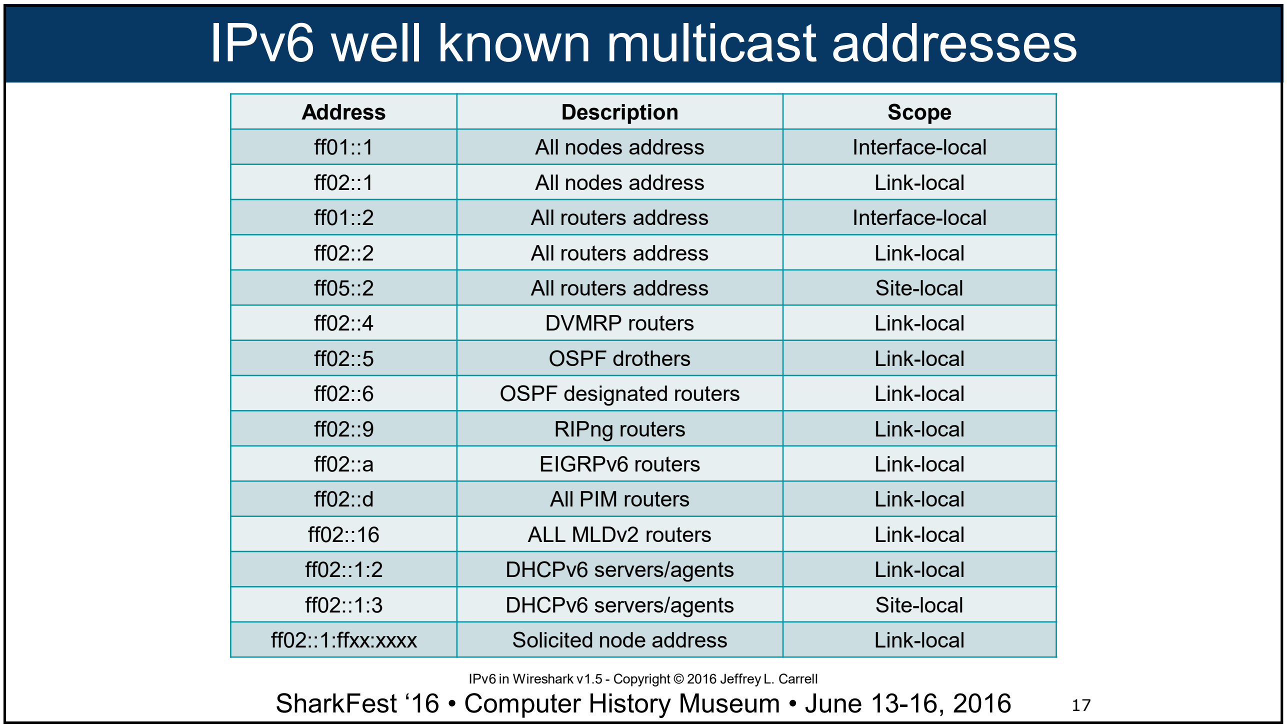
Address scopes

Address Scope	IPv4	IPv6
Link-Local - Not routable	Yes (is temp, APIPA)	Yes
Global Unicast - Routable to Internet	Aka public	Yes
Unique Local - Routable only within domain	RFC 1918 Aka private	RFC 4193



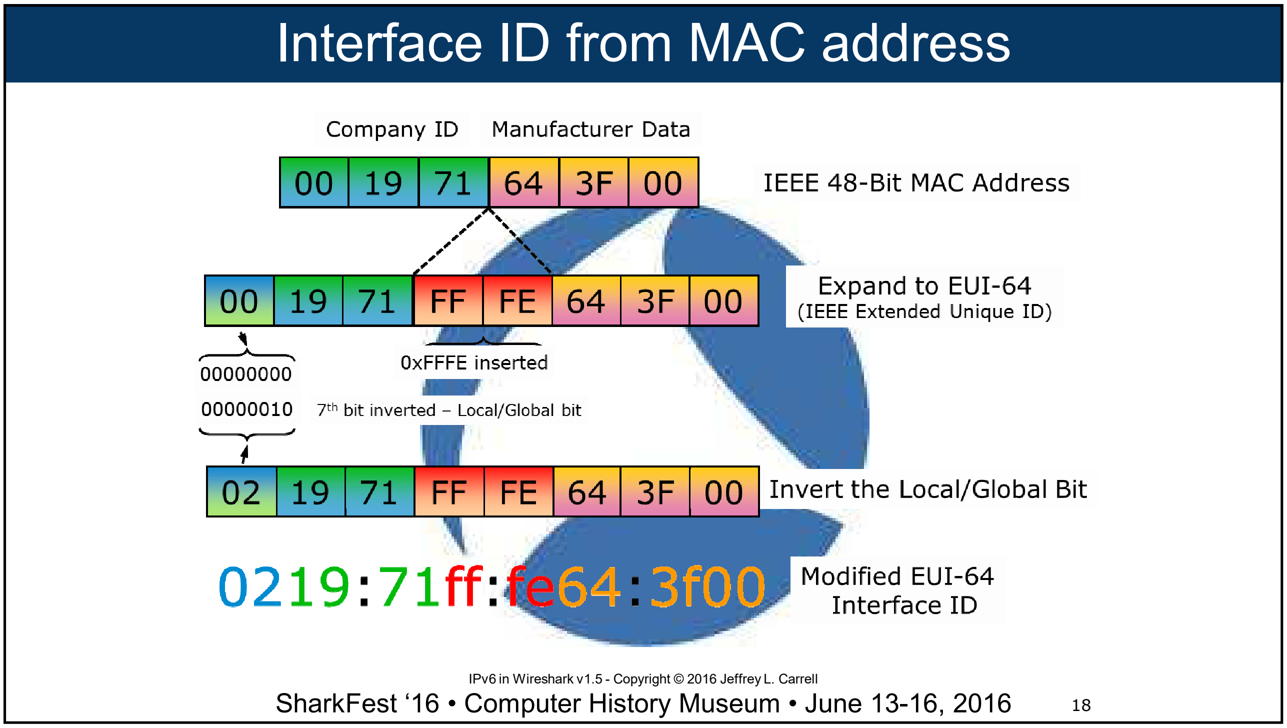
IPv4/IPv6 special addresses

Address Type	IPv4	IPv6
Default Route	0.0.0.0/0	::/0
Unspecified	0.0.0.0/32	::/128
Loopback	127.0.0.1/8	::1/128
Multicast	224.0.0.0/4	ff00::/8
Link-Local	169.254.0.0/16	fe80::/10
Global Unicast	All others	2000::/3
Unique Local	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	fc00::/7 (assigned from fd00::/8)
Documentation	192.0.2.0/24 198.51.100.0/24 203.0.113.0/24	2001:db8::/32



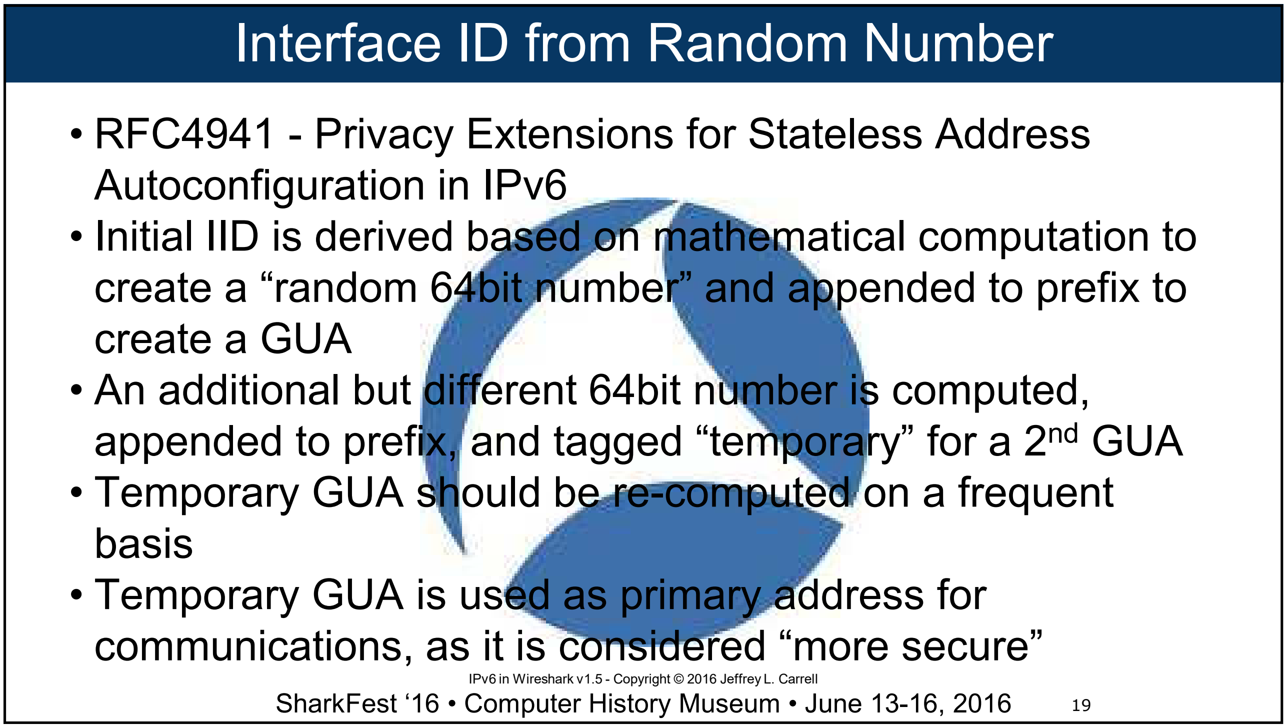
IPv6 well known multicast addresses

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



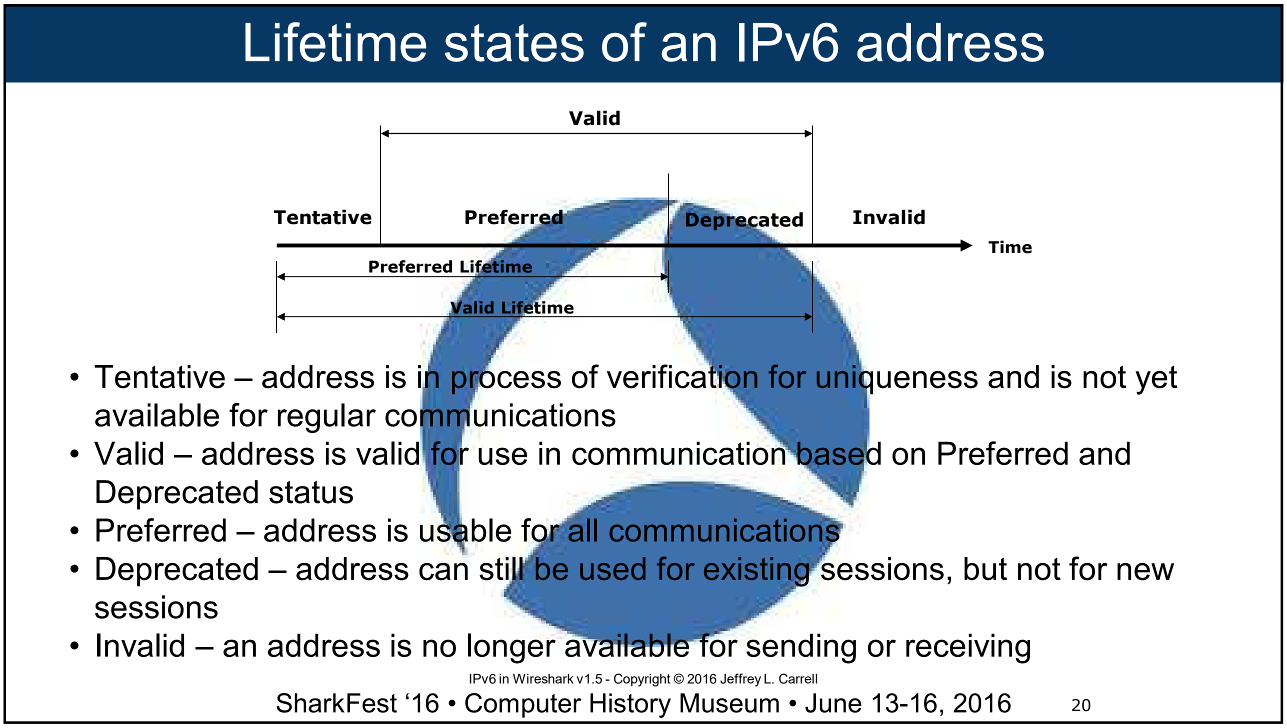
Interface ID from MAC address

Company ID
Manufacturer Data
00 | 19 | 71 | 64 | 3F | 00
IEEE 48-Bit MAC Address
00 | 19 | 71 | FF | FE | 64 | 3F | 00
Expand to EUI-64
(IEEE Extended Unique ID)
00000000
0xFFFE inserted
00000010
7th bit inverted – Local/Global bit
02 | 19 | 71 | FF | FE | 64 | 3F | 00
Invert the Local/Global Bit
0219:71ff:fe64:3f00
Modified EUI-64
Interface ID



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

Valid

Tentative

Preferred

Deprecated

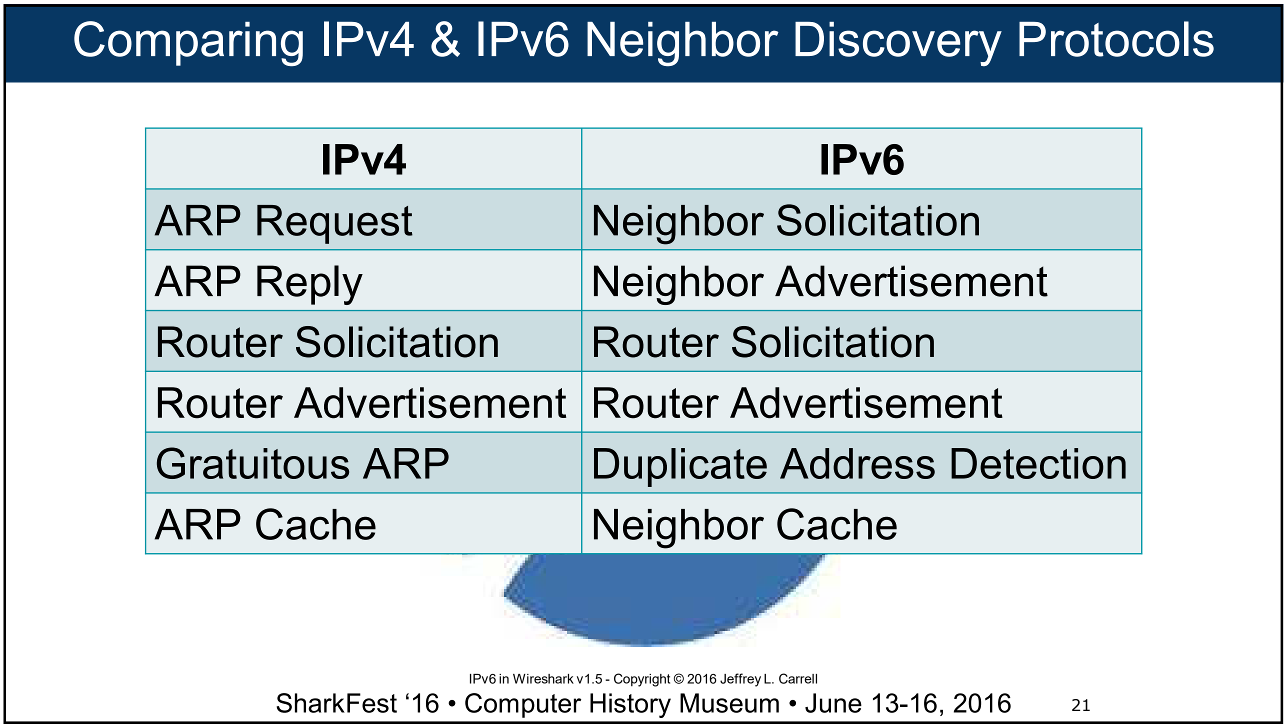
Invalid

Time

Preferred Lifetime

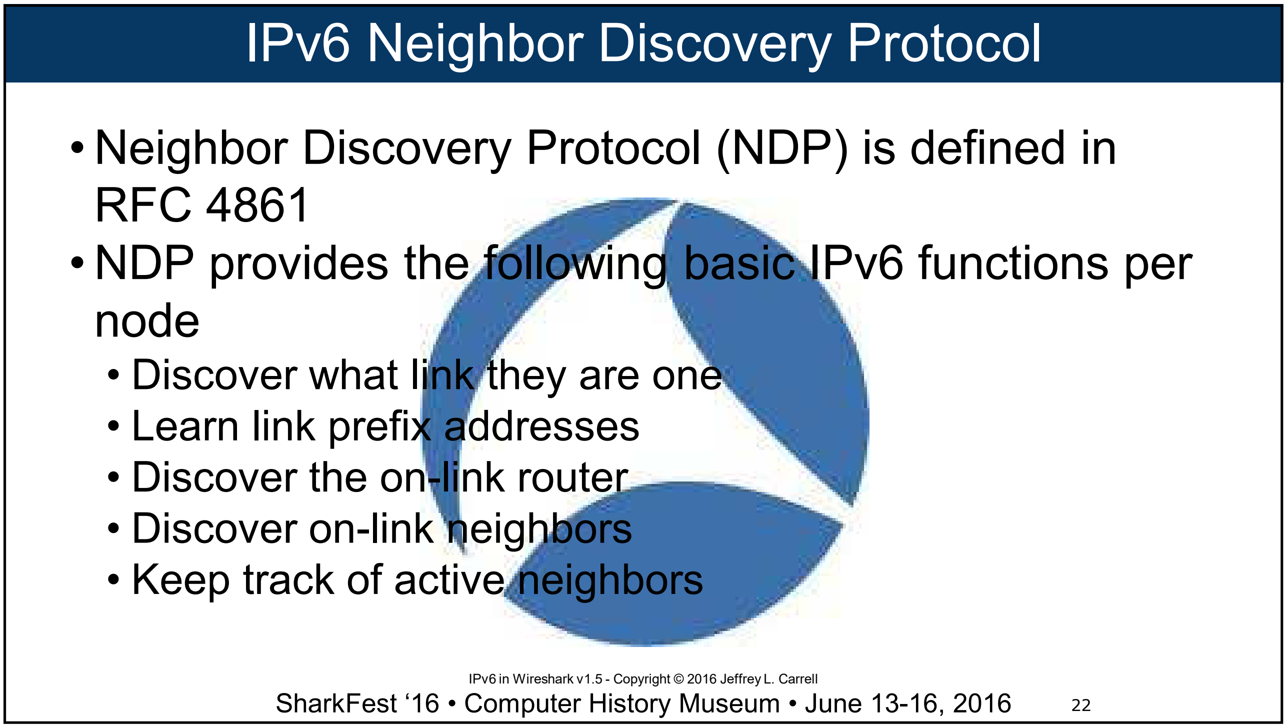
Valid Lifetime

- 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



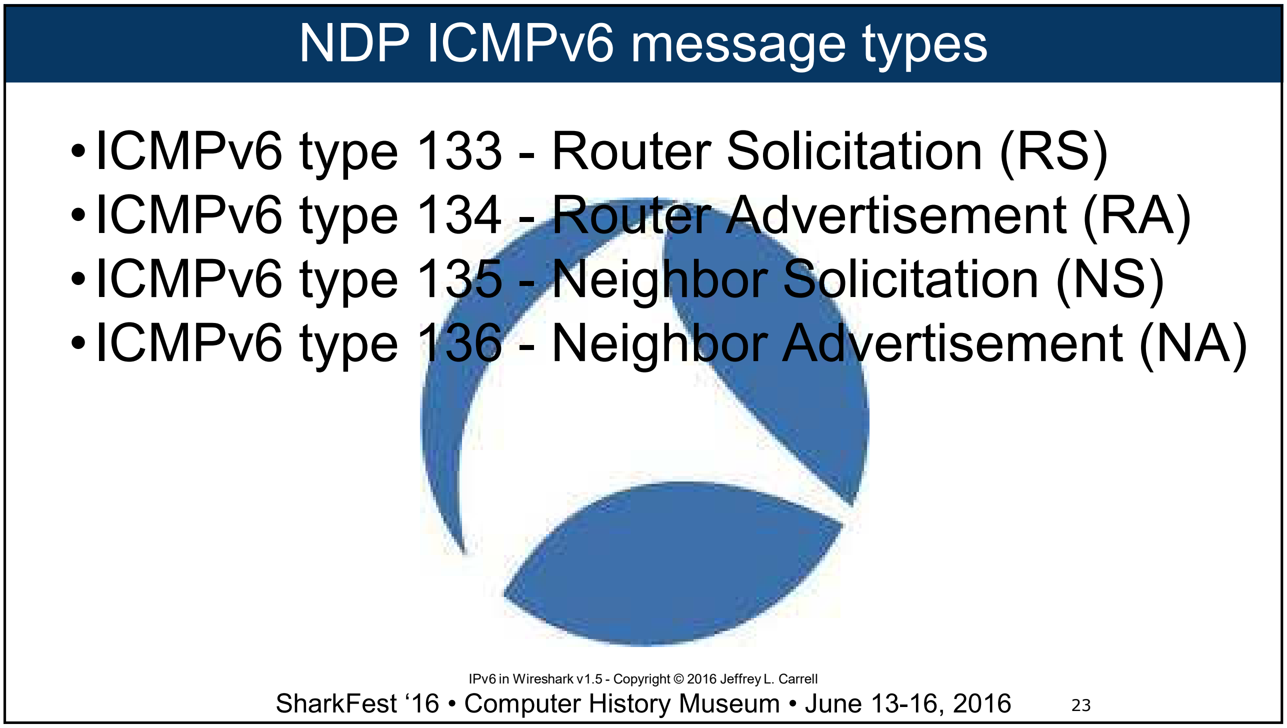
Comparing IPv4 & IPv6 Neighbor Discovery Protocols

IPv4	IPv6
ARP Request	Neighbor Solicitation
ARP Reply	Neighbor Advertisement
Router Solicitation	Router Solicitation
Router Advertisement	Router Advertisement
Gratuitous ARP	Duplicate Address Detection
ARP Cache	Neighbor Cache



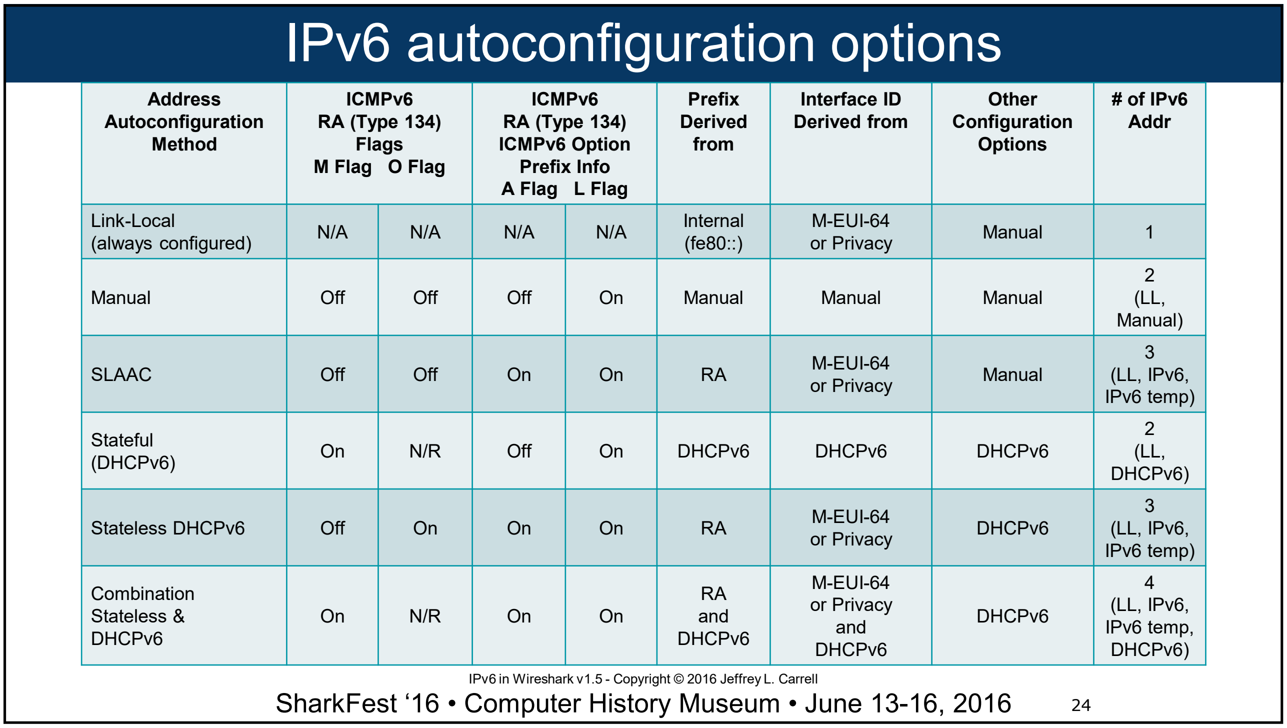
IPv6 Neighbor Discovery Protocol

- 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

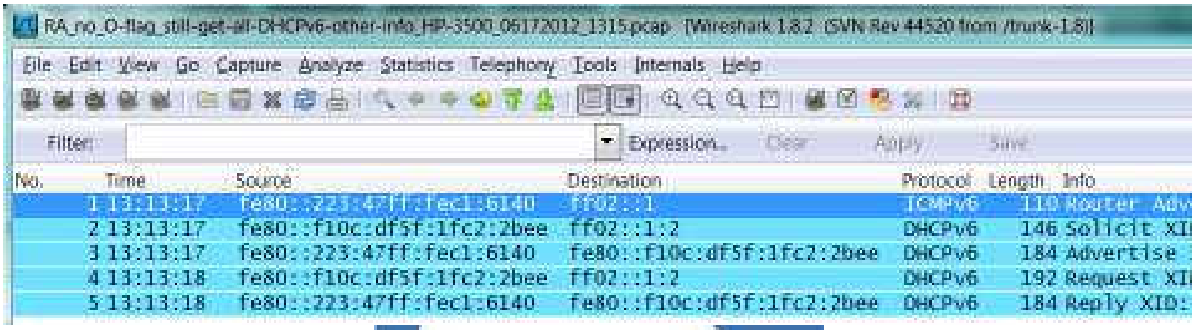
- ICMPv6 type 133 - Router Solicitation (RS)
- ICMPv6 type 134 - Router Advertisement (RA)
- ICMPv6 type 135 - Neighbor Solicitation (NS)
- ICMPv6 type 136 - Neighbor Advertisement (NA)



IPv6 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options	# of IPv6 Addr
	M Flag	O Flag	A Flag	L Flag				
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::)	M-EUI-64 or Privacy	Manual	1
Manual	Off	Off	Off	On	Manual	Manual	Manual	2 (LL, Manual)
SLAAC	Off	Off	On	On	RA	M-EUI-64 or Privacy	Manual	3 (LL, IPv6, IPv6 temp)
Stateful (DHCPv6)	On	N/R	Off	On	DHCPv6	DHCPv6	DHCPv6	2 (LL, DHCPv6)
Stateless DHCPv6	Off	On	On	On	RA	M-EUI-64 or Privacy	DHCPv6	3 (LL, IPv6, IPv6 temp)
Combination Stateless & DHCPv6	On	N/R	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6	4 (LL, IPv6, IPv6 temp, DHCPv6)

IPv6 Stateful (DHCPv6) process


RA_no_O-flag_still-get-all-DHCPv6-other-info_HP-3500_06172012_1315.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.    Time      Source                       Destination                  Protocol  Length  Info
     1 13:13:17  fe80::223:47ff:fec1:6140     ff02::1                      ICMPv6       110 Router Adv
     2 13:13:17  fe80::f10c:df5f:1fc2:2bee    ff02::1:2                    DHCPv6       146 Solicit XI
     3 13:13:17  fe80::223:47ff:fec1:6140     fe80::f10c:df5f:1fc2:2bee    DHCPv6       184 Advertise 
     4 13:13:18  fe80::f10c:df5f:1fc2:2bee    ff02::1:2                    DHCPv6       192 Request XI
     5 13:13:18  fe80::223:47ff:fec1:6140     fe80::f10c:df5f:1fc2:2bee    DHCPv6       184 Reply XID:
```

- DHCPv6**S**olicit = DHCP**D**iscover (IPv4)
- DHCPv6**A**dvertise = DHCP**O**ffer (IPv4)
- DHCPv6**R**equest = DHCP**R**equest (IPv4)
- DHCPv6**R**eply = DHCP**A**ck (IPv4)

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest ‘16 • Computer History Museum • June 13-16, 2016 25

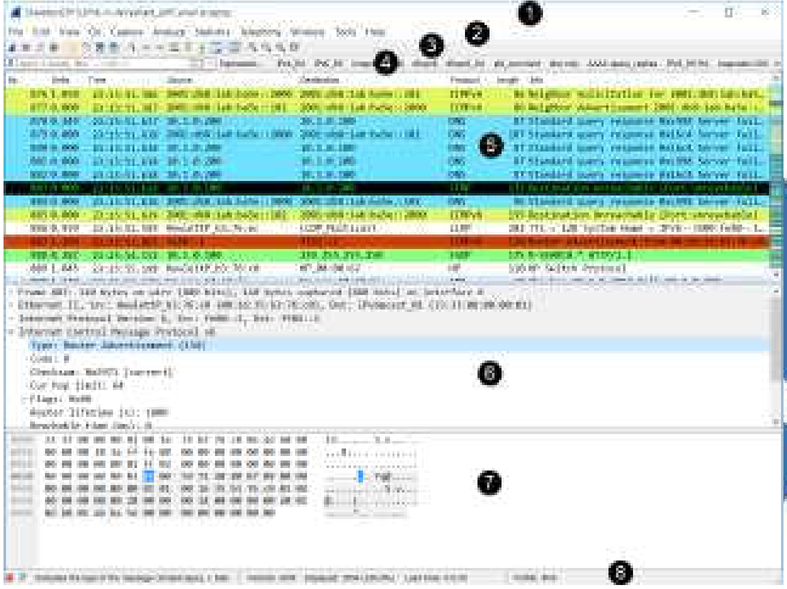
Wireshark

- Wireshark basics
- Wireshark
  - color rules
  - display filters
  - columns
  - configuration profiles
  - packet annotation
- Wireshark labs!!!

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

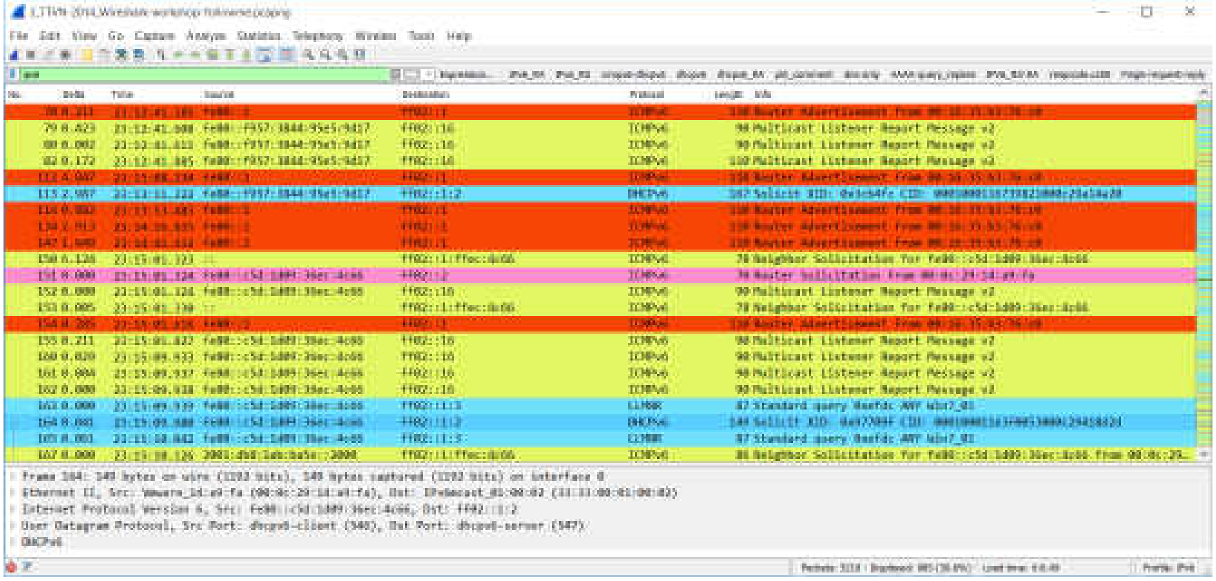
SharkFest ‘16 • Computer History Museum • June 13-16, 2016 26

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

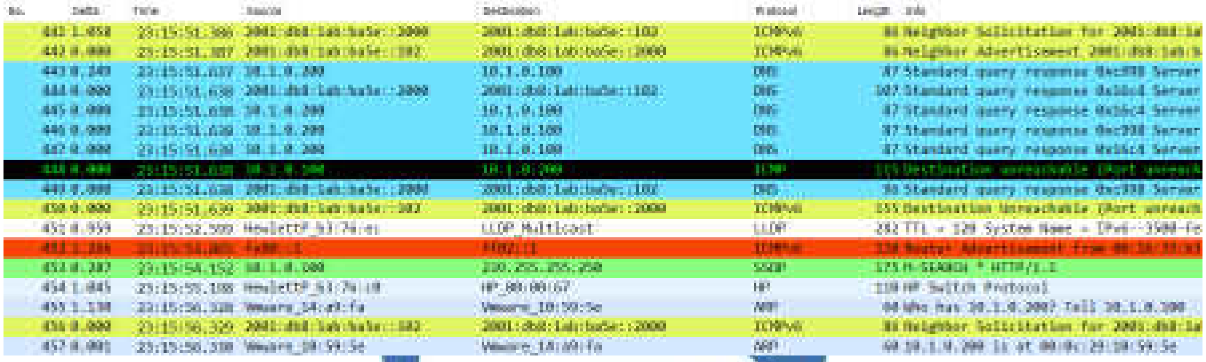
Jeff's IPv6 Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
No.  Delta  Time          Source                      Destination          Protocol  Length Info
 78 0.211  23:12:41.185  fe80::1                     ff02::1              ICMPv6    110 Router Advertisement from [illegible]
 79 0.423  23:12:41.608  fe80::f957:3844:95e5:9417   ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 80 0.002  23:12:41.611  fe80::f957:3844:95e5:9417   ff02::16             ICMPv6     90 Multicast Listener Report Message v2
 82 0.172  23:12:41.885  fe80::f957:3844:95e5:9417   ff02::16             ICMPv6    110 Multicast Listener Report Message v2
112 4.987  23:13:08.134  fe80::1                     ff02::1              ICMPv6    110 Router Advertisement from [illegible]
113 2.987  23:13:11.222  fe80::f957:3844:95e5:9417   ff02::1:2            DHCPv6    157 Solicit XID: 0x1cb4fc CID: [illegible]
114 0.882  23:13:53.485  fe80::1                     ff02::1              ICMPv6    110 Router Advertisement from [illegible]
134 2.913  23:14:15.835  fe80::1                     ff02::1              ICMPv6    110 Router Advertisement from [illegible]
147 1.640  23:14:41.432  fe80::1                     ff02::1              ICMPv6    110 Router Advertisement from [illegible]
150 6.126  23:15:01.323  ::                          ff02::1:ffoc:4c66    ICMPv6     78 Neighbor Solicitation for fe80::c5d:1d09:36ec:4c66
151 0.000  23:15:01.124  fe80::c5d:1d09:36ec:4c66    ff02::2              ICMPv6     70 Router Solicitation from 00:0c:29:1d:a9:fa
152 0.000  23:15:01.124  fe80::c5d:1d09:36ec:4c66    ff02::16             ICMPv6     90 Multicast Listener Report Message v2
153 0.005  23:15:01.130  ::                          ff02::1:ffoc:4c66    ICMPv6     78 Neighbor Solicitation for fe80::c5d:1d09:36ec:4c66
154 0.285  23:15:01.416  fe80::1                     ff02::1              ICMPv6    110 Router Advertisement from [illegible]
155 0.211  23:15:01.627  fe80::c5d:1d09:36ec:4c66    ff02::16             ICMPv6     90 Multicast Listener Report Message v2
160 0.020  23:15:09.933  fe80::c5d:1d09:36ec:4c66    ff02::16             ICMPv6     90 Multicast Listener Report Message v2
161 0.004  23:15:09.937  fe80::c5d:1d09:36ec:4c66    ff02::16             ICMPv6     90 Multicast Listener Report Message v2
162 0.000  23:15:09.938  fe80::c5d:1d09:36ec:4c66    ff02::16             ICMPv6     90 Multicast Listener Report Message v2
163 0.000  23:15:09.939  fe80::c5d:1d09:36ec:4c66    ff02::1:3            LLMNR      87 Standard query 0xefdc ANY Win7_01
164 0.001  23:15:09.940  fe80::c5d:1d09:36ec:4c66    ff02::1:2            DHCPv6    149 Solicit XID: 0x67709f CID: [illegible]
165 0.001  23:15:10.042  fe80::c5d:1d09:36ec:4c66    ff02::1:3            LLMNR      87 Standard query 0xefdc ANY Win7_01
167 0.000  23:15:10.126  2001:db8:1ab:ba5e::2000     ff02::1:ffoc:4c66    ICMPv6     86 Neighbor Solicitation for fe80::c5d:1d09:36ec:4c66 from 00:0c:29...
```

```
> Frame 164: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
> Ethernet II, Src: Vmware_1d:a9:fa (00:0c:29:1d:a9:fa), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::c5d:1d09:36ec:4c66, Dst: ff02::1:2
> User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
> DHCPv6
```

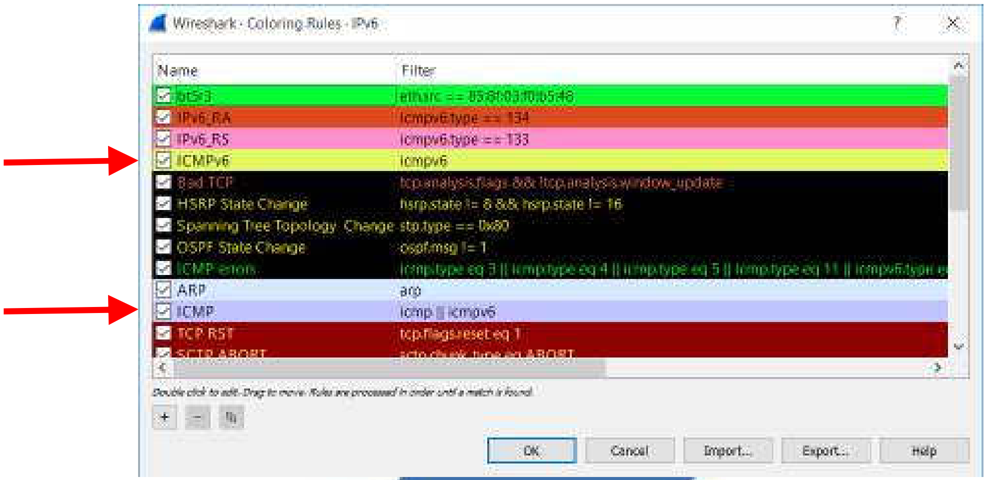
Coloring rules



```
No.  Delta  Time          Source                    Destination               Protocol  Length  Info
441  1.058  23:15:51.386  2001:db8:1ab:ba5e::2000   2001:db8:1ab:ba5e::102    ICMPv6    86  Neighbor Solicitation for 2001:db8:1a
442  0.000  23:15:51.387  2001:db8:1ab:ba5e::102    2001:db8:1ab:ba5e::2000   ICMPv6    86  Neighbor Advertisement 2001:db8:1ab:b
443  0.249  23:15:51.637  10.1.0.200                10.1.0.100                DNS       87  Standard query response 0xc098 Server
444  0.000  23:15:51.638  2001:db8:1ab:ba5e::2000   2001:db8:1ab:ba5e::102    DNS      107  Standard query response 0x1dcd Server
445  0.000  23:15:51.638  10.1.0.200                10.1.0.100                DNS       87  Standard query response 0x1dc4 Server
446  0.000  23:15:51.638  10.1.0.200                10.1.0.100                DNS       87  Standard query response 0xc098 Server
447  0.000  23:15:51.638  10.1.0.200                10.1.0.100                DNS       87  Standard query response 0x1dc4 Server
448  0.000  23:15:51.638  10.1.0.100                10.1.0.200                ICMP     115  Destination unreachable (Port unreach
449  0.000  23:15:51.638  2001:db8:1ab:ba5e::2000   2001:db8:1ab:ba5e::102    DNS       99  Standard query response 0xc098 Server
450  0.000  23:15:51.639  2001:db8:1ab:ba5e::102    2001:db8:1ab:ba5e::2000   ICMPv6   155  Destination Unreachable (Port unreach
451  0.959  23:15:52.599  HewlettP_b3:74:e1         LLDP_Multicast            LLDP     282  TTL = 120 System Name = IPv6--3500-Fe
452  1.386  23:15:54.865  fe80::1                   ff02::1                   ICMPv6   110  Router Advertisement from 00:1a:33:b3
453  0.287  23:15:54.152  10.1.0.200                239.255.255.250           SSDP     175  M-SEARCH * HTTP/1.1
454  1.045  23:15:55.198  HewlettP_b3:74:c0         HP_00:00:67               HP       110  HP Switch Protocol
455  1.130  23:15:56.328  Vmware_14:a9:fa           Vmware_10:59:5e           ARP       60  Who has 10.1.0.200? Tell 10.1.0.100
456  0.000  23:15:56.329  2001:db8:1ab:ba5e::102    2001:db8:1ab:ba5e::2000   ICMPv6    86  Neighbor Solicitation for 2001:db8:1a
457  0.001  23:15:56.330  Vmware_10:59:5e           Vmware_14:a9:fa           ARP       60  10.1.0.200 is at 00:0c:29:10:59:5e
```

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

Color rule processing order



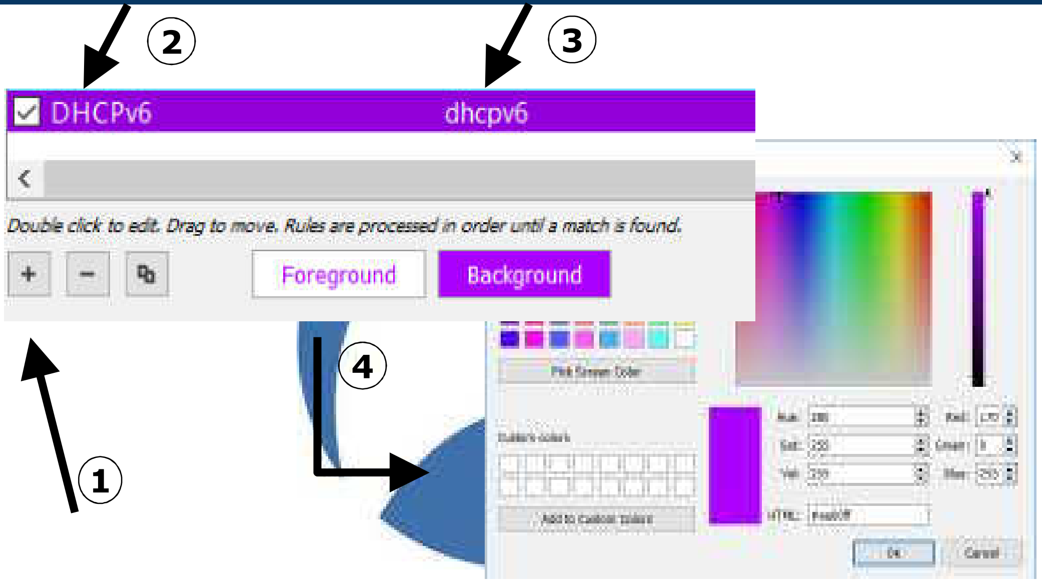
Wireshark · Coloring Rules · IPv6

Name	Filter
☑ bt5r3	eth.src == 05:8f:03:f0:b5:48
☑ IPv6_RA	icmpv6.type == 134
☑ IPv6_RS	icmpv6.type == 133
☑ ICMPv6	icmpv6
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type e
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT

Double click to edit. Drag to move. Rules are processed in order until a match is found.

- Color rules read like a router ACL or firewall rule
  - First color rule that matches wins

Color rule creation



☑ DHCPv6 dhcpv6

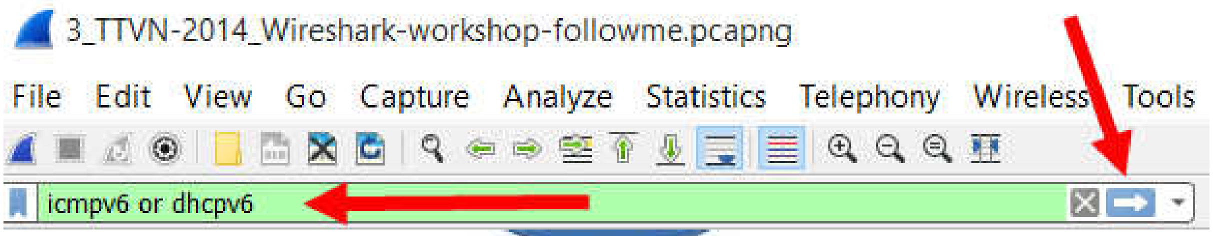
Double click to edit. Drag to move. Rules are processed in order until a match is found.

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 31

Using Wireshark to view IPv6 pkts

- IPv6 display filter families
  - ipv6
  - icmpv6
  - dhcpv6
- IPv6 related display filters:
  - http://www.wireshark.org/docs/dfref/i/ipv6.html

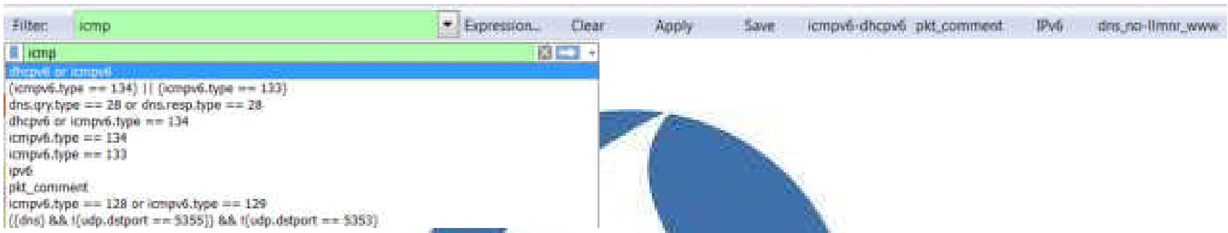


icmpv6 or dhcpv6

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 32

Display filters – option 1

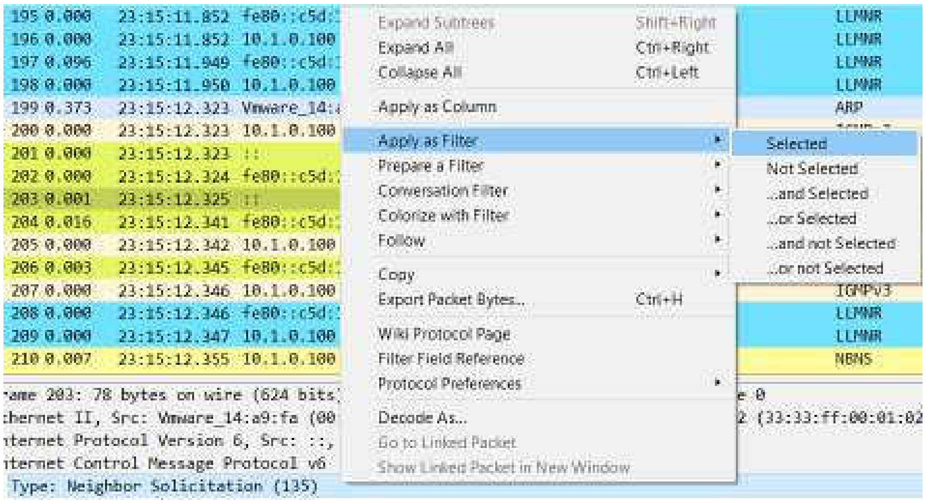


```
icmp
dhcpv6 or icmpv6
(icmpv6.type == 134) || (icmpv6.type == 133)
dns.qry.type == 28 or dns.resp.type == 28
dhcpv6 or icmpv6.type == 134
icmpv6.type == 134
icmpv6.type == 133
ipv6
pkt_comment
icmpv6.type == 128 or icmpv6.type == 129
((dns) && !(udp.dstport == 5355)) && !(udp.dstport == 5353)
```

- 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

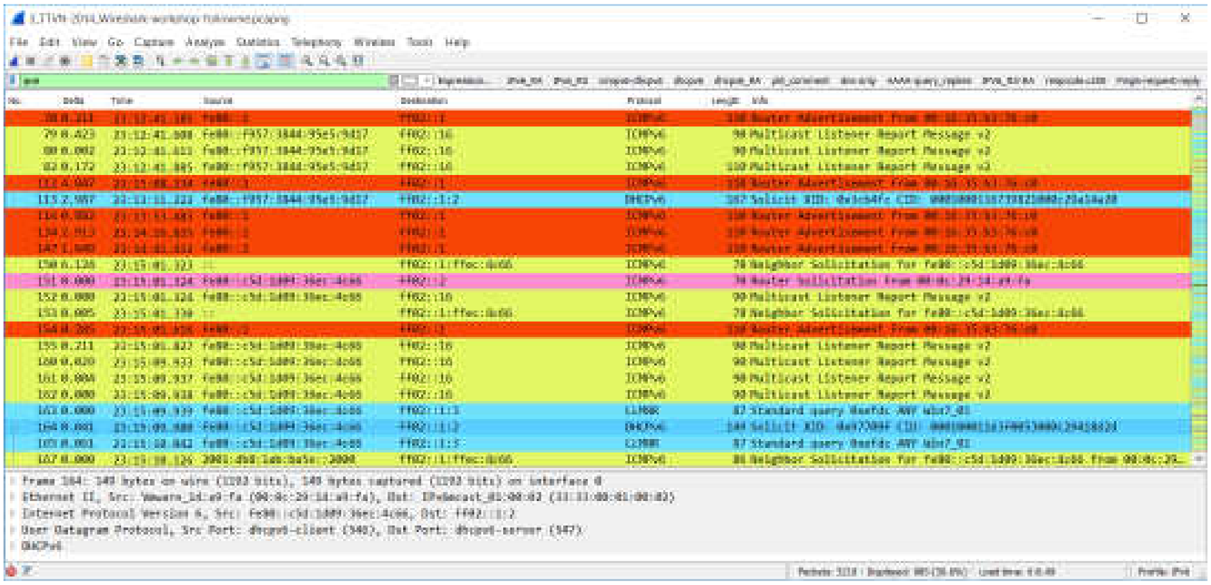
- In the Packet Details view, right-click on a specific field to build a filter



```
195 0.000   23:15:11.852 fe80::c5d:          LLMNR
196 0.000   23:15:11.852 10.1.0.100          LLMNR
197 0.096   23:15:11.949 fe80::c5d:          LLMNR
198 0.000   23:15:11.950 10.1.0.100          LLMNR
199 0.373   23:15:12.323 Vmware_14:          ARP
200 0.000   23:15:12.323 10.1.0.100
201 0.000   23:15:12.323 ::
202 0.000   23:15:12.324 fe80::c5d:
203 0.001   23:15:12.325 ::
204 0.016   23:15:12.341 fe80::c5d:
205 0.000   23:15:12.342 10.1.0.100
206 0.003   23:15:12.345 fe80::c5d:
207 0.000   23:15:12.346 10.1.0.100          IGMPv3
208 0.000   23:15:12.346 fe80::c5d:          LLMNR
209 0.000   23:15:12.347 10.1.0.100          LLMNR
210 0.007   23:15:12.355 10.1.0.100          NBNS

rame 203: 78 bytes on wire (624 bits)          e 0
thernet II, Src: Vmware_14:a9:fa (00           2 (33:33:ff:00:01:02
nternet Protocol Version 6, Src: ::,
nternet Control Message Protocol v6
 Type: Neighbor Solicitation (135)
```

Using Wireshark to view IPv6 pkts

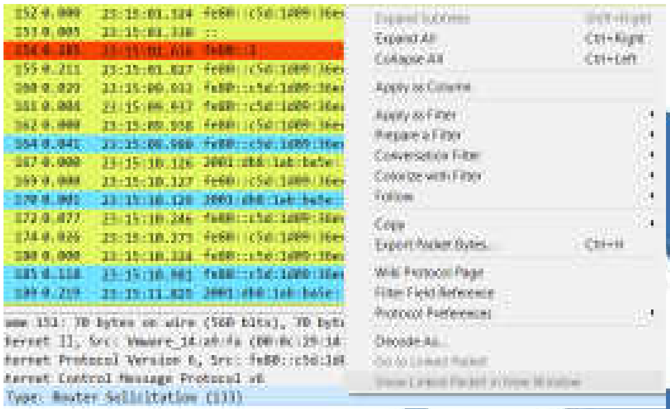

LTTVN-2014_Wireshark-workshop-fullname.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6
Expression... IPv6_RA IPv6_RS unique-dhcpv6 dhcpv6 dhcpv6_RA pd_constraint dns only AAAA query_replies IPv6_RS-RA response-LDB mcast-requests-reply

```
No.   Delta  Time          Source                     Destination         Protocol  Length Info
  78 0.211   23:12:41.185  fe80::1                    ff02::1             ICMPv6    110 Router Advertisement from 00:1b:21:53:76:c0
  79 0.423   23:12:41.608  fe80::f957:3844:95e5:9417  ff02::16            ICMPv6     90 Multicast Listener Report Message v2
  80 0.092   23:12:41.611  fe80::f957:3844:95e5:9417  ff02::16            ICMPv6     90 Multicast Listener Report Message v2
  82 0.172   23:12:41.885  fe80::f957:3844:95e5:9417  ff02::16            ICMPv6    110 Multicast Listener Report Message v2
 112 4.997   23:13:08.334  fe80::1                    ff02::1             ICMPv6    110 Router Advertisement from 00:1b:21:53:76:c0
 113 2.997   23:13:11.322  fe80::f957:3844:95e5:9417  ff02::1:2           DHCPv6    147 Solicit XID: 0x1cb4fc CID: 000100011b73352300 0c29a14a28
 116 0.092   23:13:53.403  fe80::1                    ff02::1             ICMPv6    110 Router Advertisement from 00:1b:21:53:76:c0
 134 2.913   23:14:35.835  fe80::1                    ff02::1             ICMPv6    110 Router Advertisement from 00:1b:21:53:76:c0
 147 1.080   23:14:41.112  fe80::1                    ff02::1             ICMPv6    110 Router Advertisement from 00:1b:21:53:76:c0
 150 6.126   23:15:01.323  ::                         ff02::1:ffec:4c66   ICMPv6     78 Neighbor Solicitation for fe80::c5d:1d09:36ec:4c66
 151 0.000   23:15:01.324  fe80::c5d:1d09:36ec:4c66   ff02::2             ICMPv6     70 Router Solicitation from 00:0c:29:14:a9:fa
 152 0.000   23:15:01.324  fe80::c5d:1d09:36ec:4c66   ff02::16            ICMPv6     90 Multicast Listener Report Message v2
 153 0.005   23:15:01.330  ::                         ff02::1:ffec:4c66   ICMPv6     78 Neighbor Solicitation for fe80::c5d:1d09:36ec:4c66
 154 0.285   23:15:01.616  fe80::1                    ff02::1             ICMPv6    110 Router Advertisement from 00:1b:21:53:76:c0
 155 0.211   23:15:01.827  fe80::c5d:1d09:36ec:4c66   ff02::16            ICMPv6     90 Multicast Listener Report Message v2
 160 0.020   23:15:09.933  fe80::c5d:1d09:36ec:4c66   ff02::16            ICMPv6     90 Multicast Listener Report Message v2
 161 0.004   23:15:09.937  fe80::c5d:1d09:36ec:4c66   ff02::16            ICMPv6     90 Multicast Listener Report Message v2
 162 0.000   23:15:09.938  fe80::c5d:1d09:36ec:4c66   ff02::16            ICMPv6     90 Multicast Listener Report Message v2
 163 0.000   23:15:09.939  fe80::c5d:1d09:36ec:4c66   ff02::1:3           LLMNR      87 Standard query 0xefdc ANY Win7_01
 164 0.001   23:15:09.980  fe80::c5d:1d09:36ec:4c66   ff02::1:2           DHCPv6    140 Solicit XID: 0xe7704f CID: 000100011d1f0053000c29a14a24
 165 0.001   23:15:10.042  fe80::c5d:1d09:36ec:4c66   ff02::1:3           LLMNR      87 Standard query 0xefdc ANY Win7_01
 167 0.000   23:15:10.126  2001:db8:1ab:ba5e::2000    ff02::1:ffec:4c66   ICMPv6     86 Neighbor Solicitation for fe80::c5d:1d09:36ec:4c66 from 00:0c:29…
```

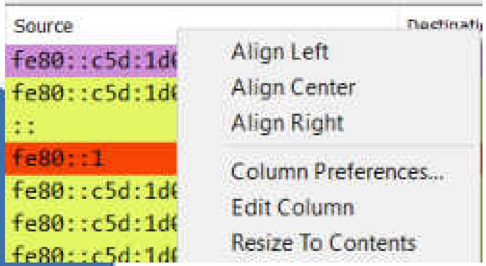
```
Frame 164: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
Ethernet II, Src: Vmware_14:a9:fa (00:0c:29:14:a9:fa), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
Internet Protocol Version 6, Src: fe80::c5d:1d09:36ec:4c66, Dst: ff02::1:2
User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
DHCPv6
```

```
Packets: 3218 · Displayed: 885 (26.8%) · Load time: 0:0.48          Profile: IPv6
```

Columns



```
152 0.000   23:15:01.124  fe80::c5d:1d09:36e
153 0.005   23:15:01.130  ::
154 0.285   23:15:01.416  fe80::1
155 0.211   23:15:01.827  fe80::c5d:1d09:36e
160 0.020   23:15:09.933  fe80::c5d:1d09:36e
161 0.004   23:15:09.937  fe80::c5d:1d09:36e
162 0.000   23:15:09.938  fe80::c5d:1d09:36e
164 0.041   23:15:09.980  fe80::c5d:1d09:36e
167 0.000   23:15:10.126  2001:db8:1ab:ba5e:
169 0.000   23:15:10.127  fe80::c5d:1d09:36e
170 0.001   23:15:10.128  2001:db8:1ab:ba5e:
172 0.477   23:15:10.246  fe80::c5d:1d09:36e
174 0.026   23:15:10.273  fe80::c5d:1d09:36e
180 0.000   23:15:10.324  fe80::c5d:1d09:36e
185 0.118   23:15:10.981  fe80::c5d:1d09:36e
189 0.219   23:15:11.825  2001:db8:1ab:ba5e:
ame 151: 70 bytes on wire (560 bits), 70 byt
ernet II, Src: Vmware_14:a9:fa (00:0c:29:14
ernet Protocol Version 6, Src: fe80::c5d:1d
ernet Control Message Protocol v6
Type: Router Solicitation (133)
```



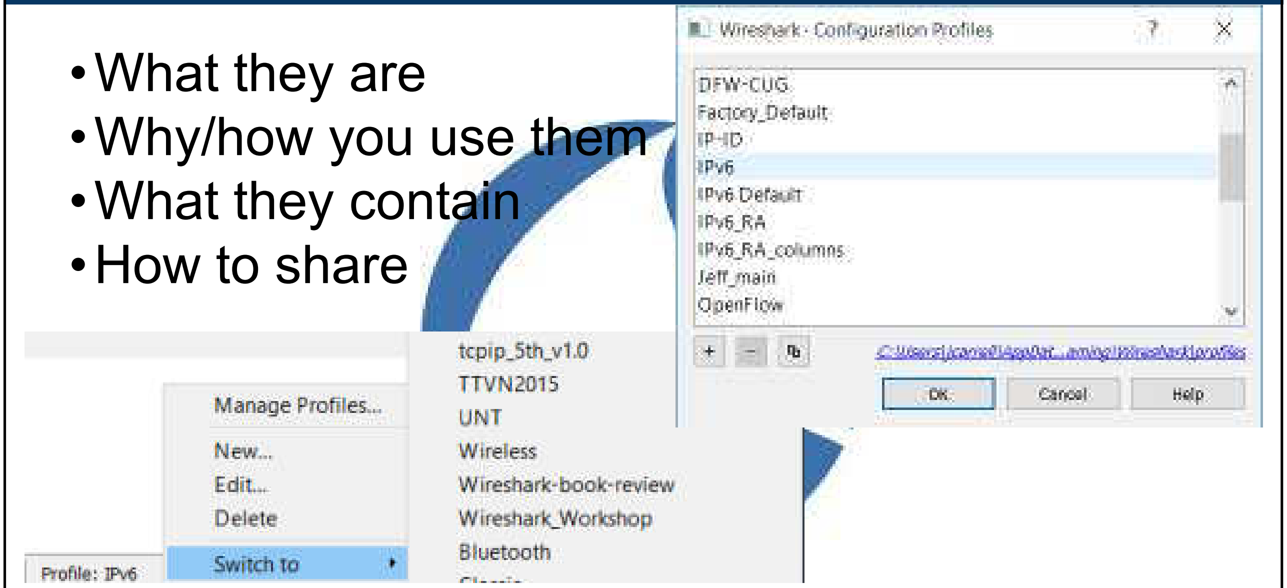
```
fe80::c5d:1d
fe80::c5d:1d
::
fe80::1
fe80::c5d:1d
fe80::c5d:1d
fe80::c5d:1d
```

- In the Packet Details view, right-click on a specific field to Apply as Column

- Right-click column headings to rename, align, etc

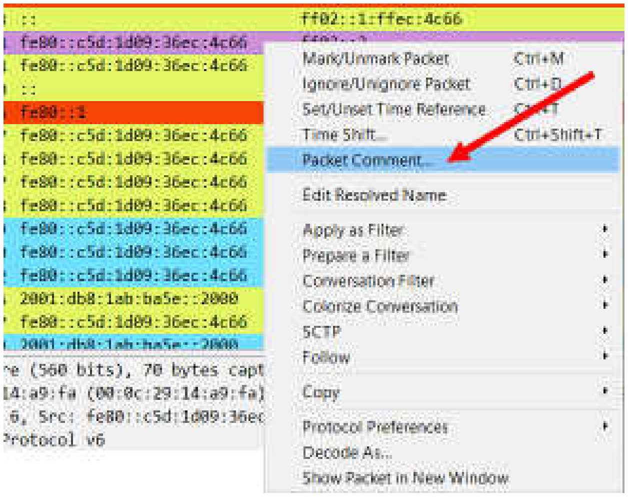
Configuration profiles

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



Packet annotation

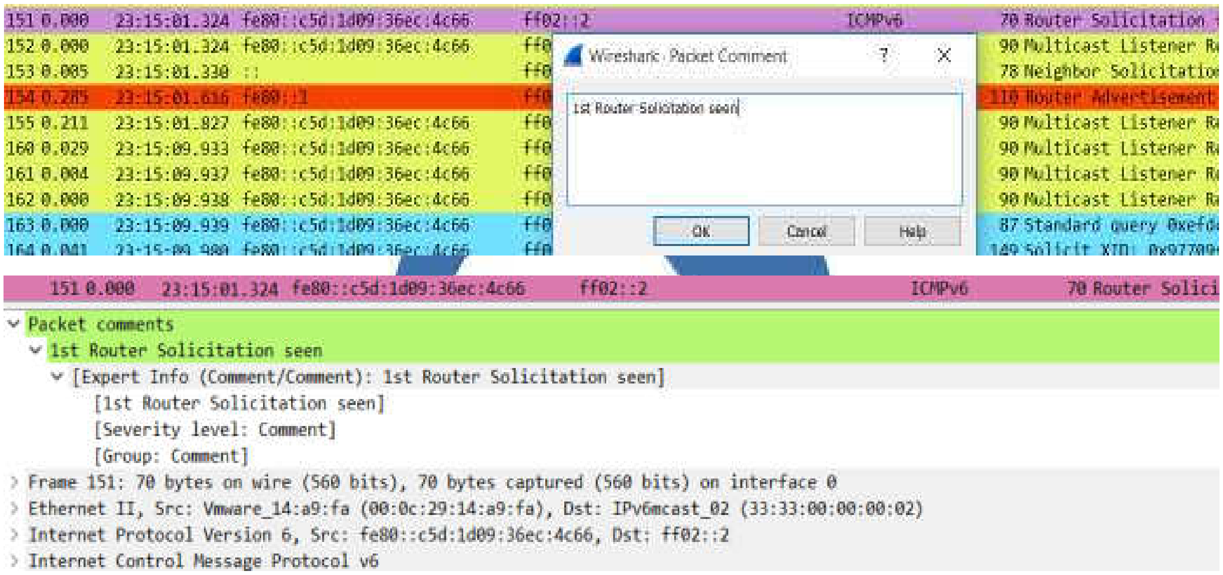
- Right click packet, select Packet Comment



```
::                            ff02::1:ffec:4c66
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
::
fe80::1
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
fe80::c5d:1d09:36ec:4c66
2001:db8:1ab:ba5e::2000
fe80::c5d:1d09:36ec:4c66
2001:db8:1ab:ba5e::2000
```

```
re (560 bits), 70 bytes capt
14:a9:fa (00:0c:29:14:a9:fa)
6, Src: fe80::c5d:1d09:36ec
Protocol v6
```

Packet annotation



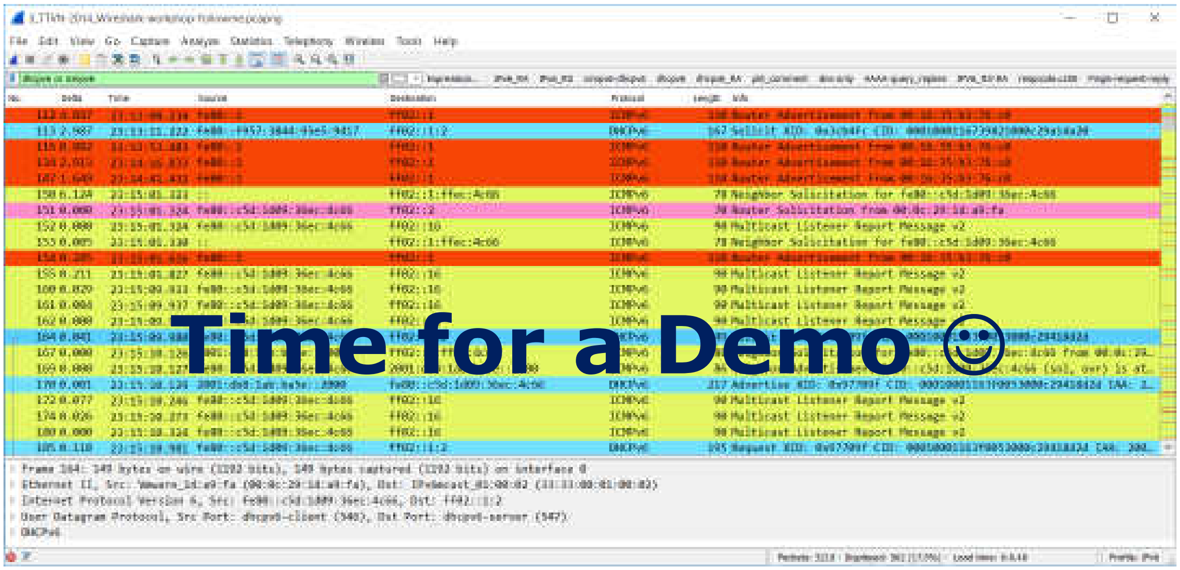
```
151 0.000   23:15:01.324 fe80::c5d:1d09:36ec:4c66   ff02::2                    ICMPv6      70 Router Solicitation
152 0.000   23:15:01.324 fe80::c5d:1d09:36ec:4c66   ff0                                    90 Multicast Listener R
153 0.005   23:15:01.330 ::                         ff0                                    78 Neighbor Solicitatio
154 0.285   23:15:01.616 fe80::1                    ff0                                   110 Router Advertisement
155 0.211   23:15:01.827 fe80::c5d:1d09:36ec:4c66   ff0                                    90 Multicast Listener R
160 0.029   23:15:09.933 fe80::c5d:1d09:36ec:4c66   ff0                                    90 Multicast Listener R
161 0.004   23:15:09.937 fe80::c5d:1d09:36ec:4c66   ff0                                    90 Multicast Listener R
162 0.000   23:15:09.938 fe80::c5d:1d09:36ec:4c66   ff0                                    90 Multicast Listener R
163 0.000   23:15:09.939 fe80::c5d:1d09:36ec:4c66   ff0                                    87 Standard query 0xefd
164 0.041   23:15:09.980 fe80::c5d:1d09:36ec:4c66   ff0                                   149 Solicit XID: 0x97709
```

Wireshark · Packet Comment

1st Router Solicitation seen

```
    151 0.000   23:15:01.324 fe80::c5d:1d09:36ec:4c66      ff02::2                 ICMPv6      70 Router Solici
∨ Packet comments
  ∨ 1st Router Solicitation seen
    ∨ [Expert Info (Comment/Comment): 1st Router Solicitation seen]
        [1st Router Solicitation seen]
        [Severity level: Comment]
        [Group: Comment]
> Frame 151: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Vmware_14:a9:fa (00:0c:29:14:a9:fa), Dst: IPv6mcast_02 (33:33:00:00:00:02)
> Internet Protocol Version 6, Src: fe80::c5d:1d09:36ec:4c66, Dst: ff02::2
> Internet Control Message Protocol v6
```

Wireshark demo #1 – watch me

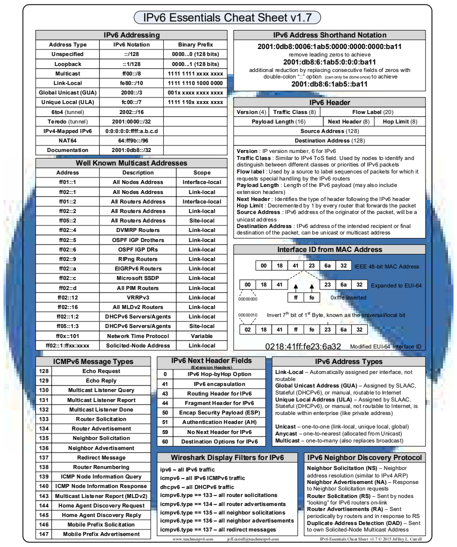


```
> Frame 164: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0
> Ethernet II, Src: Vmware_14:a9:fa (00:0c:29:14:a9:fa), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::c5d:1d09:36ec:4c66, Dst: ff02::1:2
> User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
> DHCPv6
```

Time for a Demo ☺

IPv6 Essentials Cheat Sheet

http://teachmeipv6.com/IPv6-Essentials-Cheat-Sheet.pdf



IPv6 Essentials Cheat Sheet v1.7

IPv6 Addressing

Address Type	IPv6 Notation	Binary Prefix
Unspecified	::/128	0000...0 (128 bits)
Loopback	::1/128	0000...1 (128 bits)
Multicast	ff00::/8	1111 1111 xxxx xxxx
Link-Local	fe80::/10	1111 1110 1000 0000
Global Unicast (GUA)	2000::/3	001x xxxx xxxx xxxx
Unique Local (ULA)	fc00::/7	1111 110x xxxx xxxx
6to4 (tunnel)	2002::/16	
Teredo (tunnel)	2001:0000::/32	
IPv4-Mapped IPv6	0:0:0:0:0:ffff:a.b.c.d	
NAT64	64:ff9b::/96	
Documentation	2001:0db8::/32	

Well Known Multicast Addresses

Address	Description	Scope
ff01::1	All Nodes Address	Interface-local
ff02::1	All Nodes Address	Link-local
ff01::2	All Routers Address	Interface-local
ff02::2	All Routers Address	Link-local
ff05::2	All Routers Address	Site-local
ff02::4	DVMRP Routers	Link-local
ff02::5	OSPF IGP Drothers	Link-local
ff02::6	OSPF IGP DRs	Link-local
ff02::9	RIPng Routers	Link-local
ff02::a	EIGRPv6 Routers	Link-local
ff02::c	Microsoft SSDP	Link-local
ff02::d	All PIM Routers	Link-local
ff02::12	VRRPv3	Link-local
ff02::16	All MLDv2 Routers	Link-local
ff02::1:2	DHCPv6 Servers/Agents	Link-local
ff05::1:3	DHCPv6 Servers/Agents	Site-local
ff0x::101	Network Time Protocol	Variable
ff02::1:ffxx:xxxx	Solicited-Node Address	Link-local

IPv6 Address Shorthand Notation

2001:0db8:0006:1ab5:0000:0000:0000:ba11
remove leading zeros to achieve
2001:db8:6:1ab5:0:0:0:ba11
additional reduction by replacing consecutive fields of zeros with double-colon "::" option (can only be done once) to achieve
2001:db8:6:1ab5::ba11

IPv6 Header

Version (4)	**Traffic Class** (8)	**Flow Label** (20)	
Payload Length (16)		**Next Header** (8)	**Hop Limit** (8)
Source Address (128)			
Destination Address (128)			

Version : IP version number, 6 for IPv6
Traffic Class : Similar to IPv4 ToS field. Used by nodes to identify and distinguish between different classes or priorities of IPv6 packets
Flow label : Used by a source to label sequences of packets for which it requests special handling by the IPv6 routers
Payload Length : Length of the IPv6 payload (may also include extension headers)
Next Header : Identifies the type of header following the IPv6 header
Hop Limit : Decremented by 1 by every router that forwards the packet
Source Address : IPv6 address of the originator of the packet, will be a unicast address
Destination Address : IPv6 address of the intended recipient or final destination of the packet, can be unicast or multicast address

Interface ID from MAC Address

00 | 18 | 41 | 23 | 6a | 32 IEEE 48-bit MAC Address
00 | 18 | 41 | 23 | 6a | 32 Expanded to EUI-64
00000000 ff | fe 0xfffe inserted
00000010 Invert 7th bit of 1st Byte, known as the universal/local bit
02 | 18 | 41 | ff | fe | 23 | 6a | 32
0218:41ff:fe23:6a32 Modified EUI-64 Interface ID

ICMPv6 Message Types

128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect Message
138	Router Renumbering
139	ICMP Node Information Query
140	ICMP Node Information Response
143	Multicast Listener Report (MLDv2)
144	Home Agent Discovery Request
145	Home Agent Discovery Reply
146	Mobile Prefix Solicitation
147	Mobile Prefix Advertisement

IPv6 Next Header Fields
(Extension Headers)

0	IPv6 Hop-byHop Option
41	IPv6 encapsulation
43	Routing Header for IPv6
44	Fragment Header for IPv6
50	Encap Security Payload (ESP)
51	Authentication Header (AH)
59	No Next Header for IPv6
60	Destination Options for IPv6

IPv6 Address Types

Link-Local – Automatically assigned per interface, not routable
Global Unicast Address (GUA) – Assigned by SLAAC, Stateful (DHCPv6), or manual, routable to Internet
Unique Local Address (ULA) – Assigned by SLAAC, Stateful (DHCPv6), or manual, not routable to Internet, is routable within enterprise (like private address)

Unicast – one-to-one (link-local, unique local, global)
Anycast – one-to-nearest (allocated from Unicast)
Multicast – one-to-many (also replaces broadcast)

Wireshark Display Filters for IPv6

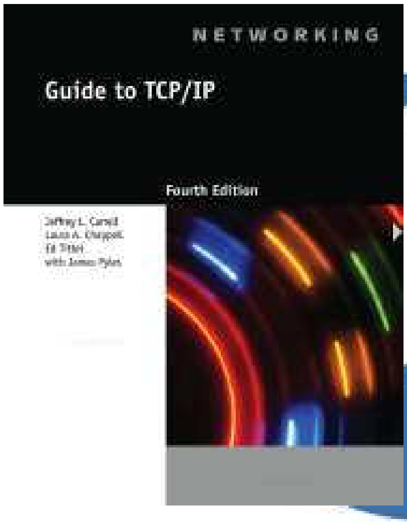
```
ipv6 – all IPv6 traffic
icmpv6 – all IPv6 ICMPv6 traffic
dhcpv6 – all DHCPv6 traffic
icmpv6.type == 133 – all router solicitations
icmpv6.type == 134 – all router advertisements
icmpv6.type == 135 – all neighbor solicitations
icmpv6.type == 136 – all neighbor advertisements
icmpv6.type == 137 – all redirect messages
```

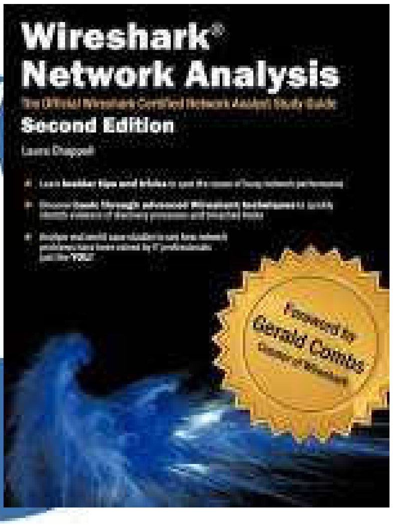
IPv6 Neighbor Discovery Protocol

Neighbor Solicitation (NS) – Neighbor address resolution (similar to IPv4 ARP)
Neighbor Advertisement (NA) – Response to Neighbor Solicitation requests
Router Solicitation (RS) – Sent by nodes "looking" for IPv6 routers on-link
Router Advertisements (RA) – Sent periodically by routers and in response to RS
Duplicate Address Detection (DAD) – Sent to own Solicited-Node Multicast Address

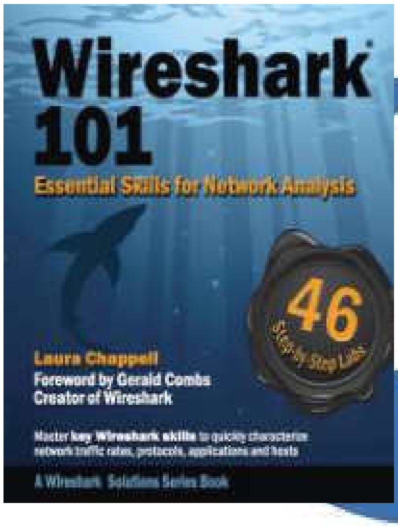
www.teachmeipv6.com jeff.carrell@teachmeipv6.com IPv6 Essentials Cheat Sheet v1.7 © 2015 Jeffrey L. Carrell

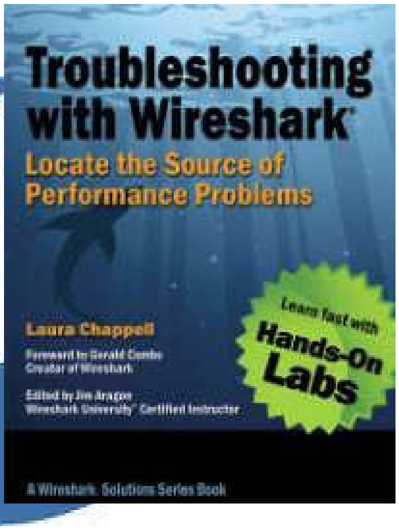
Resources



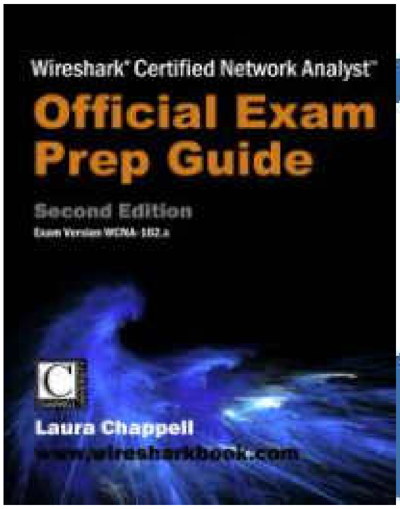

Wireshark®
Network Analysis
The Official Wireshark Certified Network Analyst Study Guide
Second Edition
Laura Chappell
Foreword by Gerald Combs Creator of Wireshark

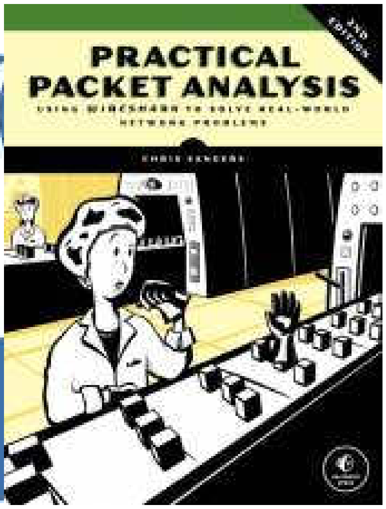
Resources


Wireshark 101
Essential Skills for Network Analysis
46 Step-by-Step Labs
Laura Chappell
Foreword by Gerald Combs
Creator of Wireshark
Master key Wireshark skills to quickly characterize network traffic rates, protocols, applications and hosts
A Wireshark Solutions Series Book

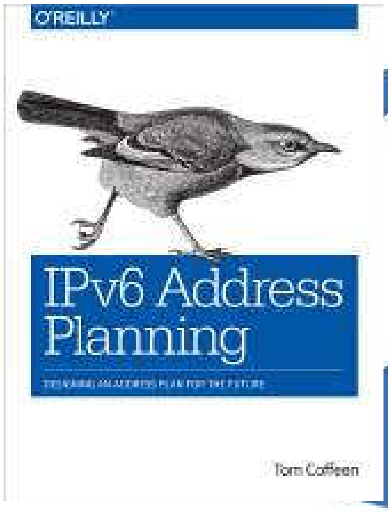

Troubleshooting with Wireshark
Locate the Source of Performance Problems
Learn fast with Hands-On Labs
Laura Chappell
Foreword by Gerald Combs
Creator of Wireshark
Edited by Jim Aragon
Wireshark University Certified Instructor
A Wireshark Solutions Series Book

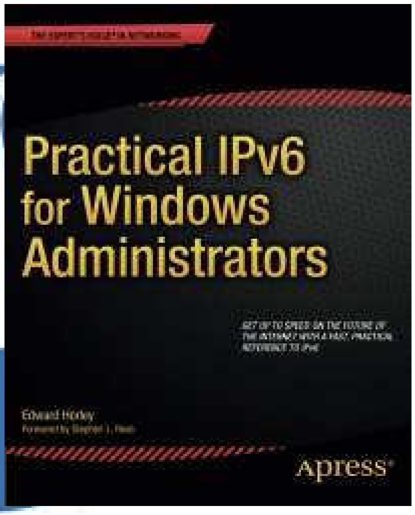
Resources




2ND EDITION
PRACTICAL PACKET ANALYSIS
USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS
CHRIS SANDERS

Resources

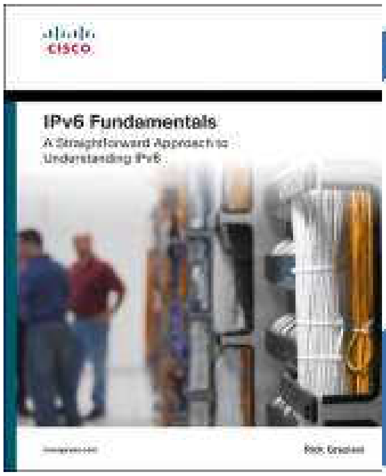


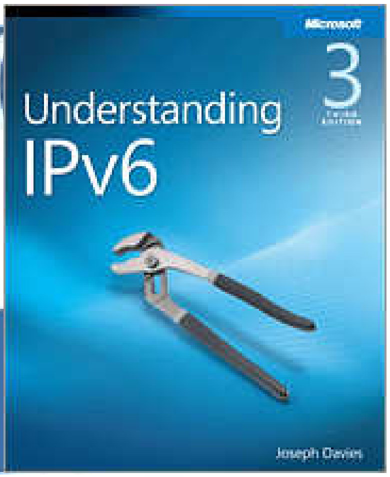


IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 45

Resources

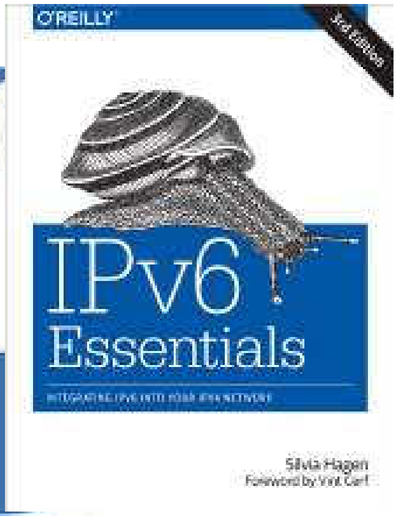




IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 46

Resources



IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 47

Thank You for Attending!

jeff.carrell@teachmeipv6.com

Twitter: @JeffCarrell_v6

Certificate of Completion

jeffcarrell

hereby awarded the rank of

Sage

Hurricane Electric
IPv6 Certification

IPv6 in Wireshark v1.5 - Copyright © 2016 Jeffrey L. Carrell

SharkFest '16 • Computer History Museum • June 13-16, 2016 48