

Troubleshooting IPv6 in Wireshark

Troubleshooting IPv6 in Wireshark

Jeffrey L Carrell

Network Trainer

jeff.carrell@teachmeipv6.com

Twitter: @JeffCarrell_v6



IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

1

IPv6 in Wireshark

- IPv6 – a very quick review
- Wireshark basics
- Wireshark color rules, display filters, columns, configuration profiles, and packet annotation
- IPv6 in Wireshark: hands-on labs

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

2

Troubleshooting IPv6 in Wireshark



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

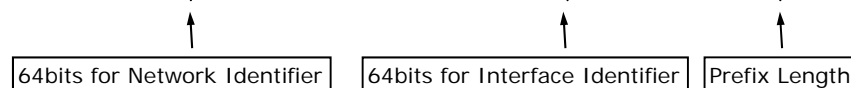
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

3



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

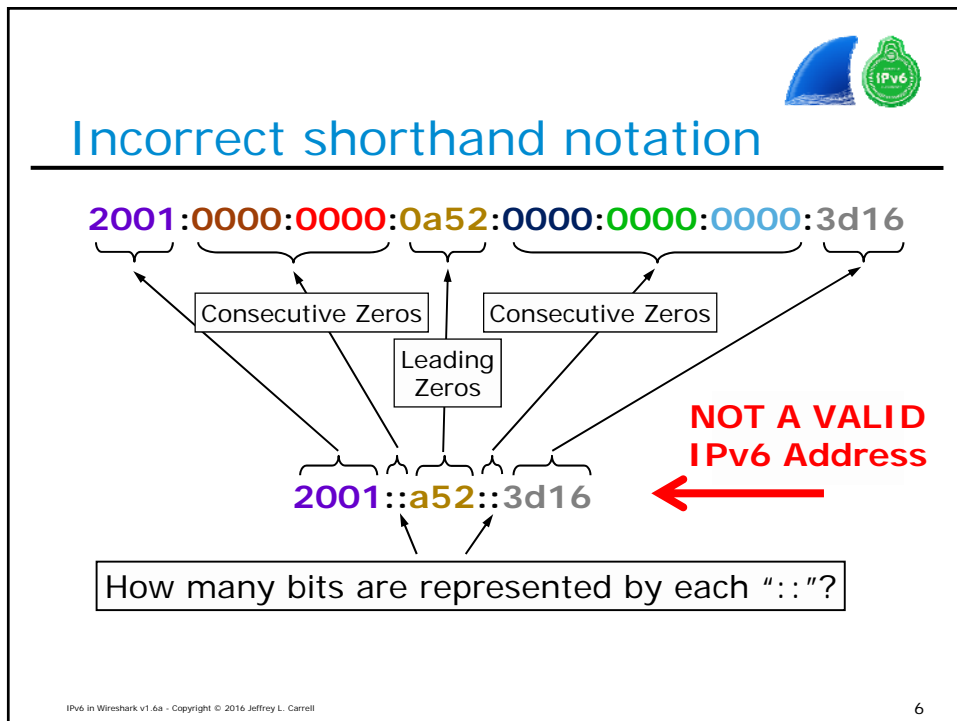
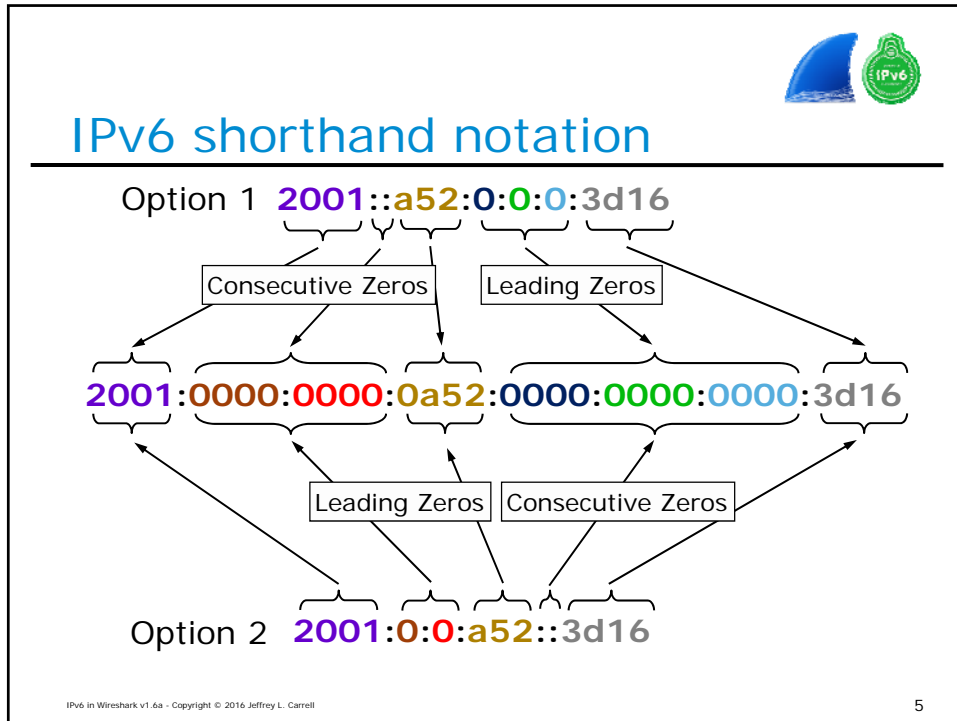


- A single /64 network yields 18 billion-billion possible addresses

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

4

Troubleshooting IPv6 in Wireshark



Troubleshooting IPv6 in Wireshark



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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

7




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
Documentation	192.0.2.0/24 198.51.100.0/24 203.0.113.0/24	2001:db8::/32

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

8

Troubleshooting IPv6 in Wireshark

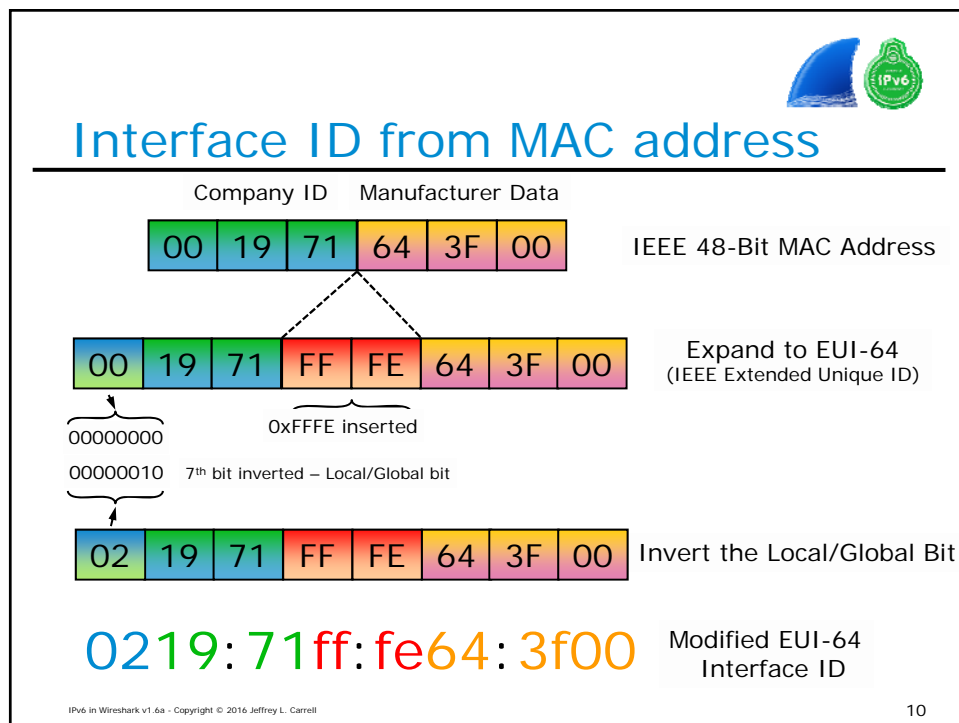


IPv6 well known multicast addresses

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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

9



Troubleshooting IPv6 in Wireshark



Interface ID from Random Number

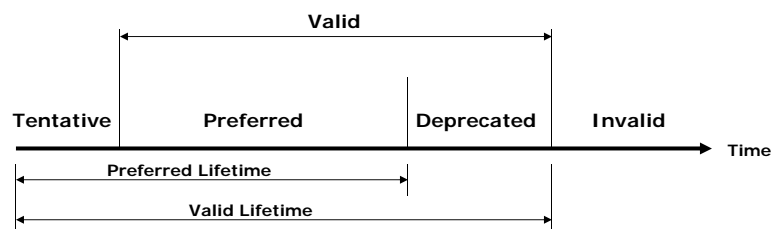
- RFC4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- Initial IID is derived based on mathematical computation to create a "random 64bit number" and appended to prefix to create a GUA
- An additional but different 64bit number is computed, appended to prefix, and tagged "temporary" 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"

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

11



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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

12

Troubleshooting IPv6 in Wireshark



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 on
 - Learn link prefix addresses
 - Discover the on-link router
 - Discover on-link neighbors
 - Keep track of active neighbors

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

13



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 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

14

Troubleshooting IPv6 in Wireshark



Duplicate Address Detection (DAD)

- When a node initially assigns an IPv6 address to its interface, it must check whether the selected address is unique
- If unique, the address is configured on interface
- To verify uniqueness, the node sends a multicast Neighbor Solicitation message with the:
 - dest MAC of 33:33:<last 32bits of IPv6 mcast addr>
 - dest IPv6 addr of ff02::1:ff<last 24bits of proposed IPv6 addr>
 - source IPv6 of "::" (IPv6 unspecified addr)

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

15





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)

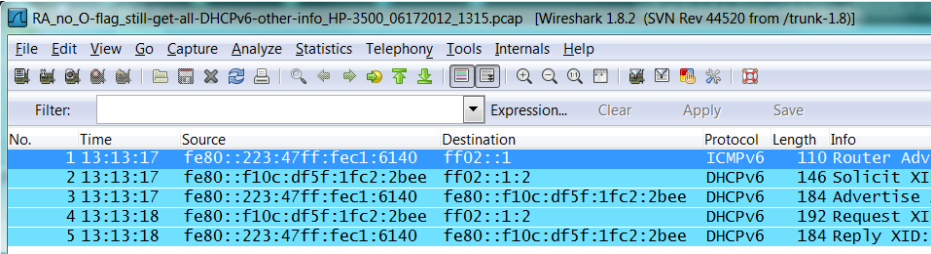
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

16

Troubleshooting IPv6 in Wireshark



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 XI

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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

17



Wireshark

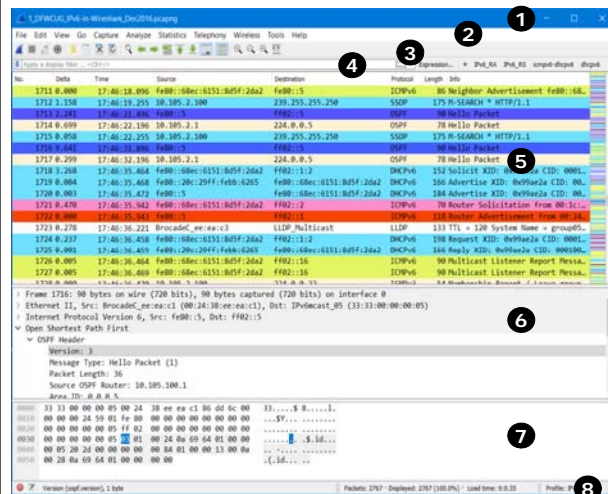
- Wireshark basics
- Wireshark
 - color rules
 - display filters
 - columns
 - configuration profiles
 - packet annotation
- Wireshark labs!!!

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

18

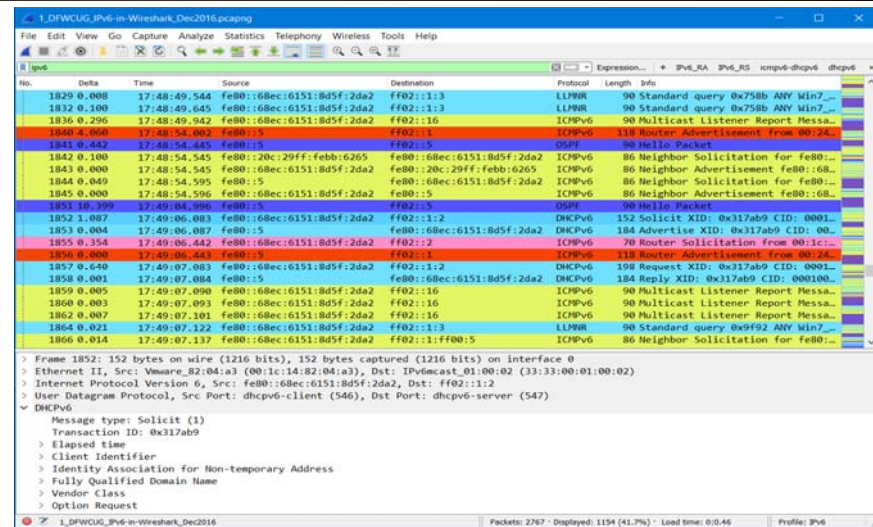
Troubleshooting IPv6 in Wireshark

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



Troubleshooting IPv6 in Wireshark

Coloring rules



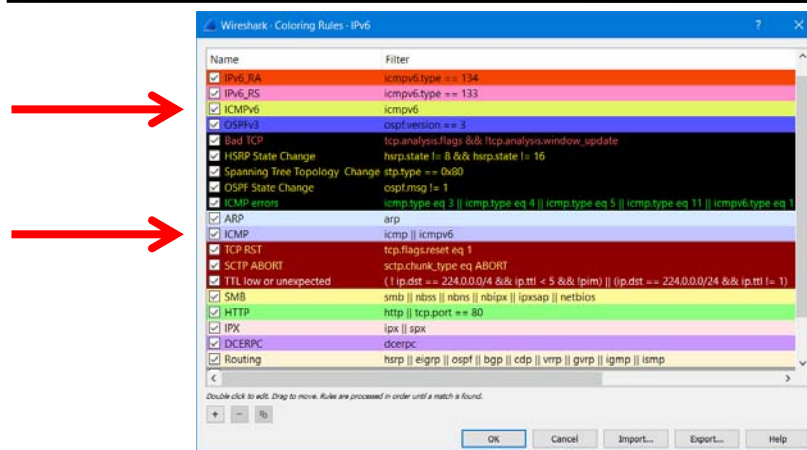
1710 0.062	17:46:18.096	fe80::5	fe80::68ec:6151:8d5f:2da2	ICMPv6	86 Neighbor Solicitation for fe80::68ec:6151:8d5f:2da2
1711 0.000	17:46:18.096	fe80::68ec:6151:8d5f:2da2	fe80::5	ICMPv6	86 Neighbor Advertisement fe80::68ec:6151:8d5f:2da2
1712 1.158	17:46:19.255	10.105.2.100	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1713 2.241	17:46:21.496	fe80::5	ff02::5	OSPF	90 Hello Packet
1714 0.699	17:46:22.196	10.105.2.1	224.0.0.5	OSPF	78 Hello Packet
1715 0.058	17:46:22.255	10.105.2.100	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1716 9.641	17:46:31.896	fe80::5	ff02::5	OSPF	90 Hello Packet
1717 0.299	17:46:32.196	10.105.2.1	224.0.0.5	OSPF	78 Hello Packet
1718 3.268	17:46:35.464	fe80::68ec:6151:8d5f:2da2	ff02::1:2	DHCPv6	152 Solicit XID: 0x99ae2a CID: 0001000115e...
1719 0.004	17:46:35.468	fe80::20c:29ff:febb:6265	fe80::68ec:6151:8d5f:2da2	DHCPv6	166 Advertise XID: 0x99ae2a CID: 0001000115e...
1720 0.003	17:46:35.472	fe80::5	fe80::68ec:6151:8d5f:2da2	DHCPv6	184 Advertise XID: 0x99ae2a CID: 0001000115e...
1721 0.470	17:46:35.942	fe80::68ec:6151:8d5f:2da2	ff02::2	ICMPv6	70 Router Solicitation from 00:1c:14:82:0:0
1722 0.000	17:46:35.943	fe80::5	ff02::1	ICMPv6	118 Router Advertisement from 00:24:38:ee:0:0
1723 0.278	17:46:36.221	Brocade_c_ea:c3	LLDP_Multicast	LLDP	133 TTL = 120 System Name = group05_NetIron
1724 0.237	17:46:36.458	fe80::68ec:6151:8d5f:2da2	ff02::1:2	DHCPv6	198 Request XID: 0x99ae2a CID: 0001000115e...
1725 0.001	17:46:36.459	fe80::20c:29ff:febb:6265	fe80::68ec:6151:8d5f:2da2	DHCPv6	166 Reply XID: 0x99ae2a CID: 0001000115e87...
1726 0.005	17:46:36.464	fe80::68ec:6151:8d5f:2da2	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
1727 0.005	17:46:36.469	fe80::68ec:6151:8d5f:2da2	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
1728 0.000	17:46:36.470	10.105.2.100	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0.0.22

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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

21

Color rule processing order



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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

22

Troubleshooting IPv6 in Wireshark

Color rule creation

1 2 3 4

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

23

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>

1_DFWCUG_IPv6-in-Wireshark_Dec2016.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcpv6 or icmpv6

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

24

Troubleshooting IPv6 in Wireshark



Display filters – option 1

```
dhcpv6 or icmpv6
ipv6
http.response.code == 200
dhcpv6 or icmpv6.type == 134
ssh
dhcpv6 or icmpv6
icmpv6.type == 134 || (icmpv6.type == 133)
quic or dns
quic
icmpv6.type == 134
icmpv6.type == 128 or icmpv6.type == 129
```

- 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

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell 25



Display filters – option 2

No.	Time	Source	Destination
193	0.000	17:05:16.614 10.105.2.100	224.0.0.252
194	0.327	17:05:16.942 10.105.2.100	224.0.0.22
195	0.000	17:05:16.942 ::	ff02::1:ff00:107
196	0.000	17:05:16.942 fe80::68ec:6151:8d5f:2da2	ff02::16
197	0.017	17:05:16.959 fe80::68ec:6151:8d5f:2da2	ff02::16
198	0.000	17:05:16.959 10.105.2.100	224.0.0.22
199	0.004	17:05:16.964 fe80::68ec:6151:8d5f:2da2	ff02::16
200	0.000	17:05:16.964 10.105.2.100	224.0.0.22
201	0.001	17:05:16.966 fe80::68ec:6151:8d5f:2da2	ff02::1:3

> Frame 195: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: Vmware_82:04:a3 (00:1c:14:82:04:a3), Dst: IPv6mcast_ff:00:01:07 (33:33:ff:00:01:07)
> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff00:107

▼ Internet Control Message Protocol v6

Type: Neighbor Solicitation (135)

Code: 0
Checksum: 0x83d2 [correct]
[Checksum Status: Good]
Reserved: 00000000
Target Address: 2001:470:ba04:1652::107

Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy



Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

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

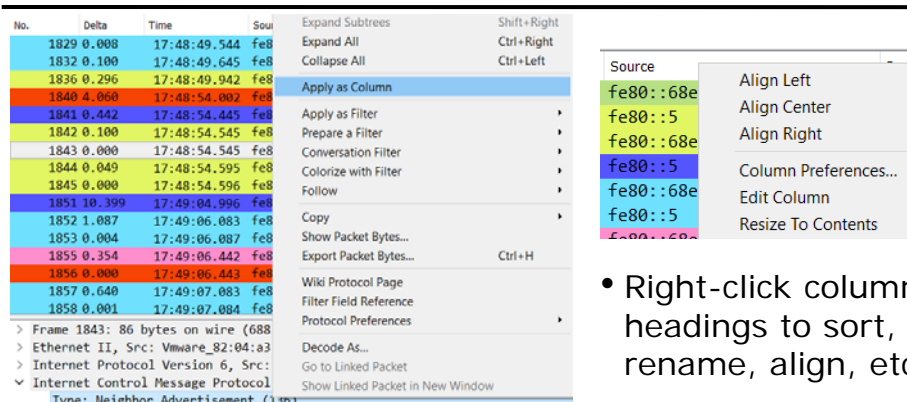
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

26

Troubleshooting IPv6 in Wireshark



Columns





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

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

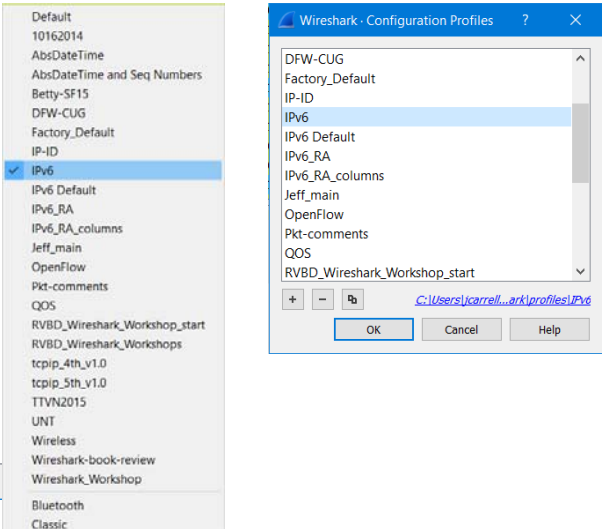
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

27



Configuration profiles

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



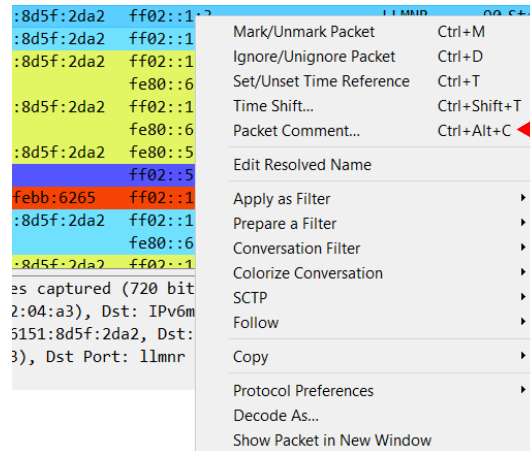
Profile: IPv6

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

28

Troubleshooting IPv6 in Wireshark

Packet annotation

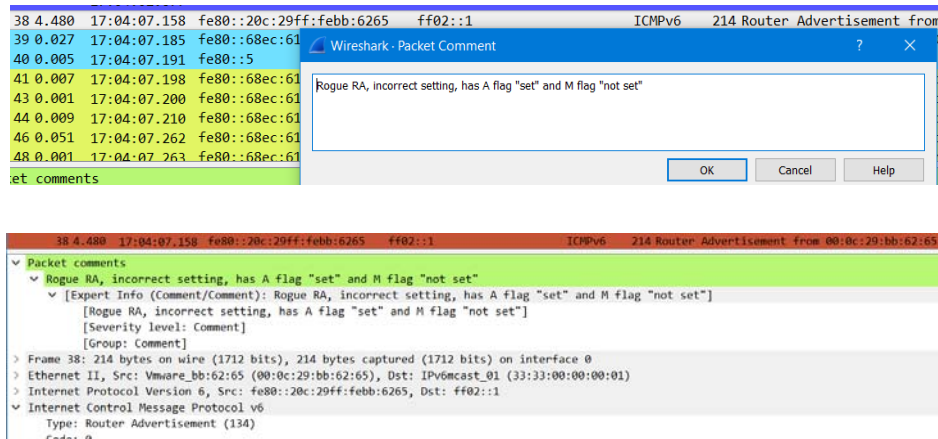


- Right click packet, select Packet Comment

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

29

Packet annotation

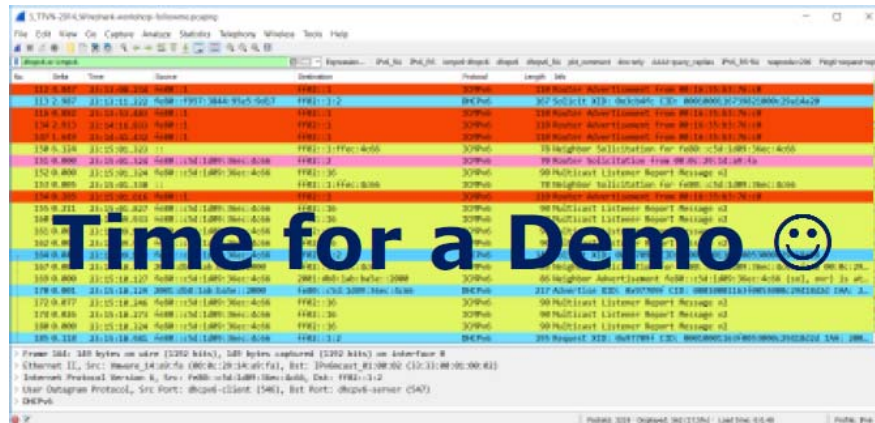


IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

30

Troubleshooting IPv6 in Wireshark

Wireshark demo #1 – watch me



IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

31

Wireshark lab #1 - setup

- Open:
"2_IPv6-in-Wireshark_Feb2017.pcapng"
- Create your own named profile
- Add delta time column
- Change time/date to time (only) and in milliseconds
- Turn off Packet Bytes

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

32

Troubleshooting IPv6 in Wireshark



Wireshark lab #2 - DNS

- Find 1st pkt with dns.qry.name == "www.ipv6sandbox.com"
 - make a note as to which pkt this is _____
- Find 1st pkt with DNS query response for www.ipv6sandbox.com
 - make a note as to which pkt this is _____
 - what is the IPv6 address in the answer section _____

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

33



Wireshark lab #3 - HTTP

- Find pkt with http.host == "www.ipv6sandbox.com"
 - make a note as to which pkt this is _____
- Find pkt with an http response code of 200
 - make a note as to which pkt this is _____

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

34

Troubleshooting IPv6 in Wireshark



Wireshark lab #4 – IPv6-RA

- Inspect RA packets
 - configure a display filter as
"icmpv6.type == 134"
 - which flags are set to "1" in this RA:
M ____ O ____ L ____ A ____
 - which IPv6 address autoconfiguration option
is this RA configured for?
SLAAC ____ Stateful(DHCPv6) ____ Stateless DHCPv6 ____

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

35



Wireshark lab #5 – DHCPv6

- Inspect DHCPv6 packets
 - configure a display filter as "dhcpv6"
 - pick a specific client
 - find the first pkt of each of its DHCPv6 process
 - what are the pkt numbers for:
Solicit ____ Advertise ____ Request ____ Reply ____
 - what is the dhcpv6 server's v6 addr?

 - what v6 address did the client get assigned?

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

36

Troubleshooting IPv6 in Wireshark



Wireshark lab #5 – DHCPv6

- How to find rogue DHCPv6 servers
 - configure a display filter as `dhcpv6.msgtype == 2`
 - look for more DHCPv6 Advertisement sources than you expect to see

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

37



Wireshark lab #6 – rogue router?

- Open:
 - “1_IPv6-in-Wireshark_Feb2017.pcapng”
- Inspect RA packets
 - configure a display filter as `icmpv6.type == 134`
- How many IPv6 routers do you see? _____
 - what prefixes are they advertising?
- Which one do you think is not right (a rogue)?
- Add columns for M,O,A,L Prefix for quicker analysis

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

38

Troubleshooting IPv6 in Wireshark



Wireshark lab #6 – rogue router

- You will be configuring a specific display filter to view a portion of an IPv6 prefix which contains "2bad" in the 4th hextet. It has previously been determined that this configuration of a network prefix is not correct for this network
 - `ipv6.src[6:2] == 2b:ad`
 - 2001:db8:74c:2bad

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

39



Wireshark lab #6 – bad prefix

- In pkt 1915, the client attempts to ping a valid IP6 address for google.com.
 - How did it know what was the correct address?
 - Did the DNS reply back to the client on IPv6?
- What is happening, why does it look like it is working – kinda????

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

40

Troubleshooting IPv6 in Wireshark

Wireshark lab #7 – did you see that



- Look for all clients sending AAAA query. Scroll through the list and view both IPv4 and IPv6 clients making and replying to these queries. Specifically view if any IPv6 clients are making AAAA queries
 - `dns-qry.type == 28`
 - Do you see something interesting, if so, what was it? _____

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

41

Wireshark lab #8 – lots of prefixes



- Now using pkt 1911, configure display filter on source MAC address
- View all the different IPv4 and IPv6 associated with this MAC address
- How many different IPv6 addresses are associated with this MAC address? _____
 - Why is this occurring?

IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

42

Troubleshooting IPv6 in Wireshark

IPv6 Essentials Cheat Sheet

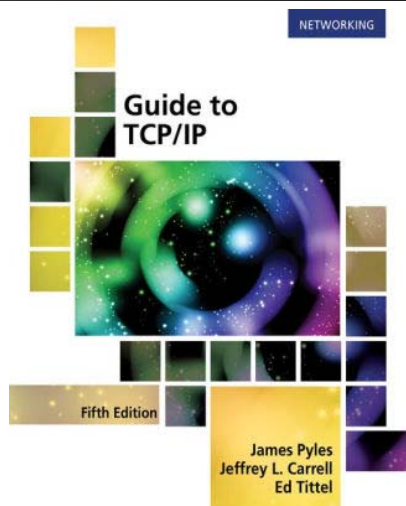
<http://teachmeipv6.com/IPv6-Essentials-Cheat-Sheet.pdf>

[illegible]

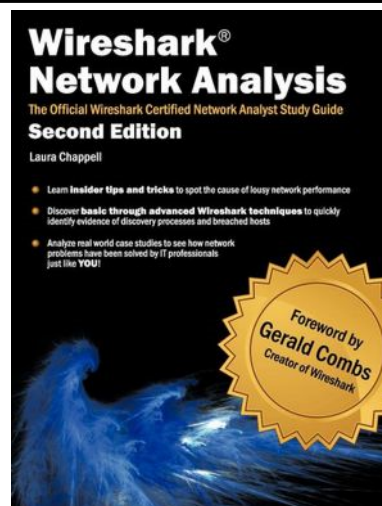
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrel

43

Resources



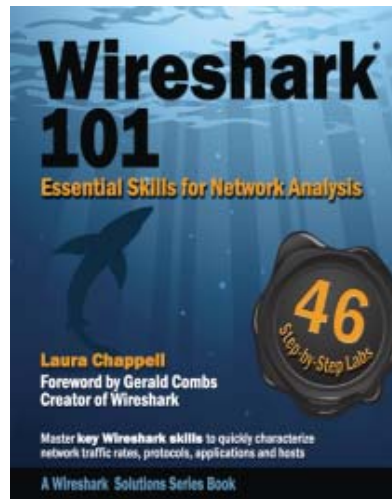
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrel



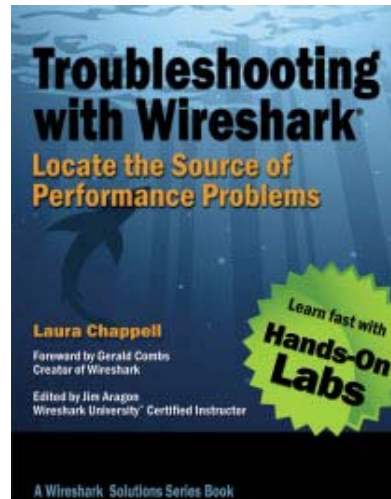
44

Troubleshooting IPv6 in Wireshark

Resources

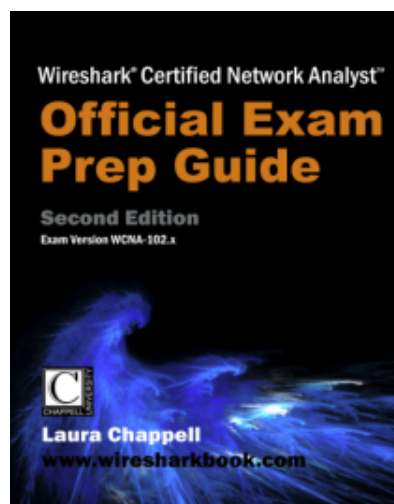


IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

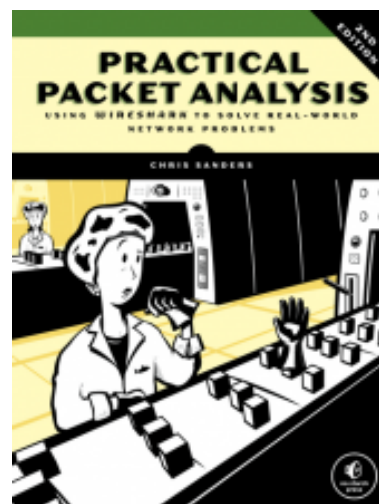


45

Resources



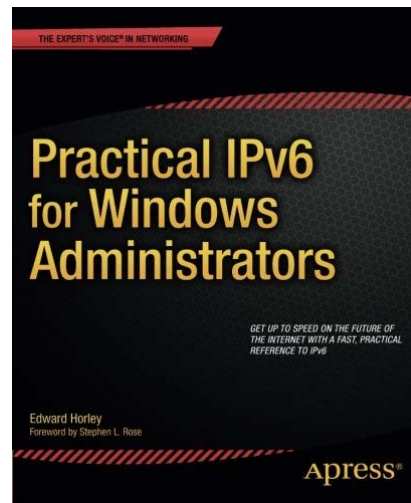
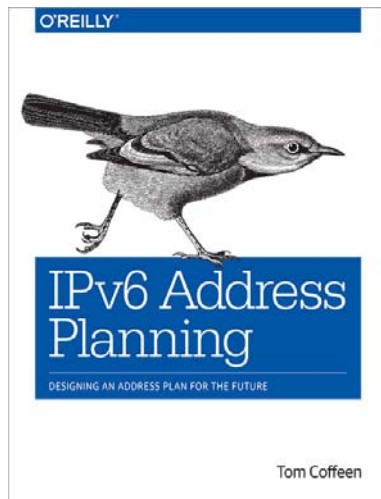
IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell



46

Troubleshooting IPv6 in Wireshark

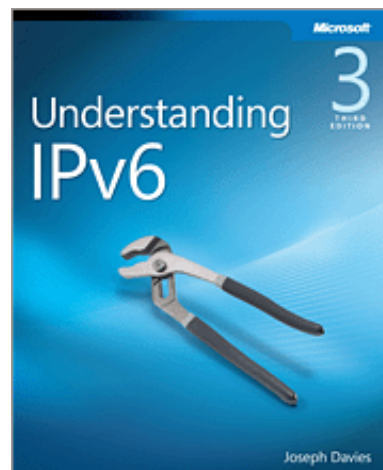
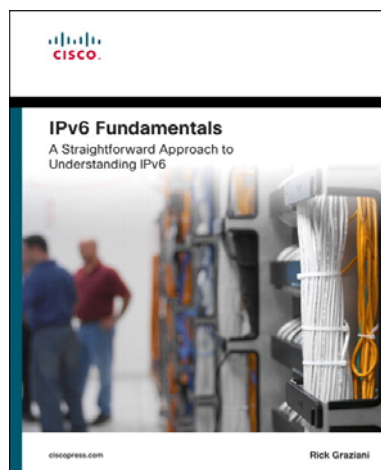
Resources



IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

47

Resources

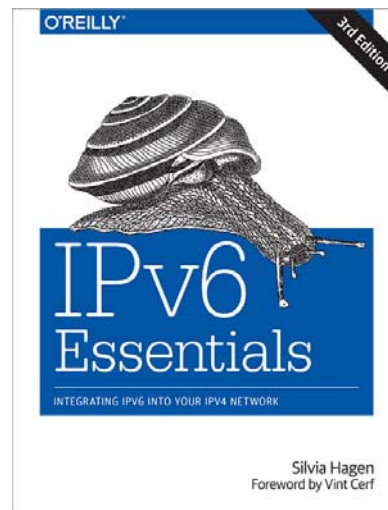


IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

48

Troubleshooting IPv6 in Wireshark

Resources



IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

49

Thank You for Attending!



- jeff.carrell@teachmeipv6.com
- Twitter: @JeffCarrell_v6



IPv6 in Wireshark v1.6a - Copyright © 2016 Jeffrey L. Carrell

50