download trace file - https://app.box.com/sharkfest2015

IPv6 in Wireshark

Jeffrey L Carrell

Network Conversions

Network Consultant
IPv6 SME/Trainer

jeff.carrell@teachmeipv6.com

Twitter: @JeffCarrell_v6

2

download trace file - https://app.box.com/sharkfest2015

IPv6 in Wireshark

- IPv6 "briefly"
- Wireshark basics
- Wireshark color rules, display filters, columns and configuration profiles

IPv6 - briefly

- Quick IPv6 history
- IPv6 Address basics
- IPv6 Address Autoconfiguration
- DCHPv6 and DNS for IPv6

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?

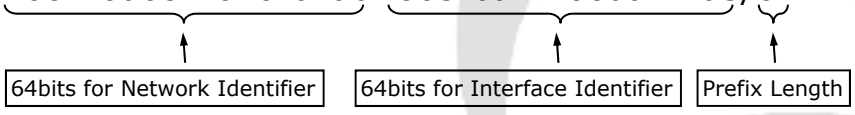
- IPv6 addresses are very different than IPv4 addresses in the size, numbering system, and delimiter between the numbers
  - 128bit -vs- 32bit
  - hexadecimal -vs- decimal
  - colon and double colon -vs- period (or "dot" for the real geeks)
- Valid IPv6 addresses are comprised of hexadecimal numbers (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

7

IPv6 default for subnet

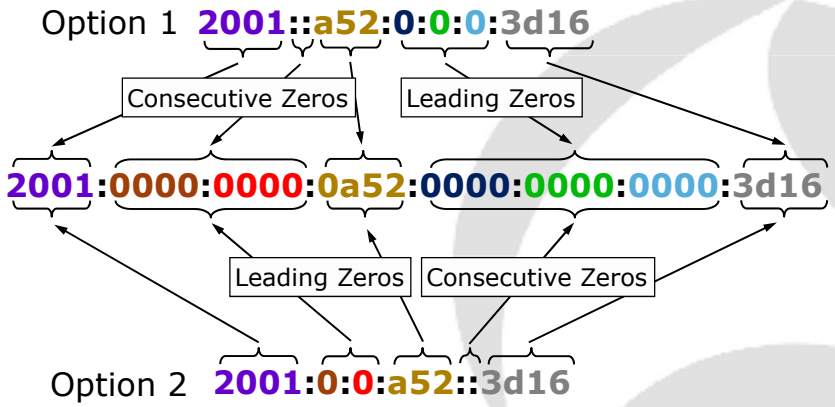
- Based on the default definition an IPv6 address is logically divided into two parts: a 64-bit network prefix and a 64-bit interface identifier (IID)
- Therefore, the default subnet size is /64
- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64



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

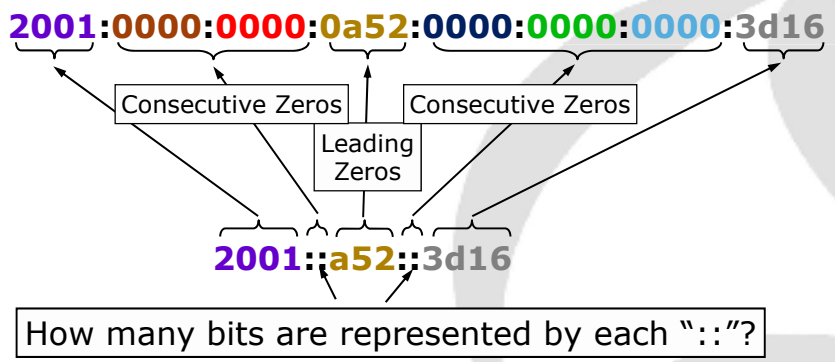
8

IPv6 shorthand notation



9

Incorrect shorthand notation



10

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

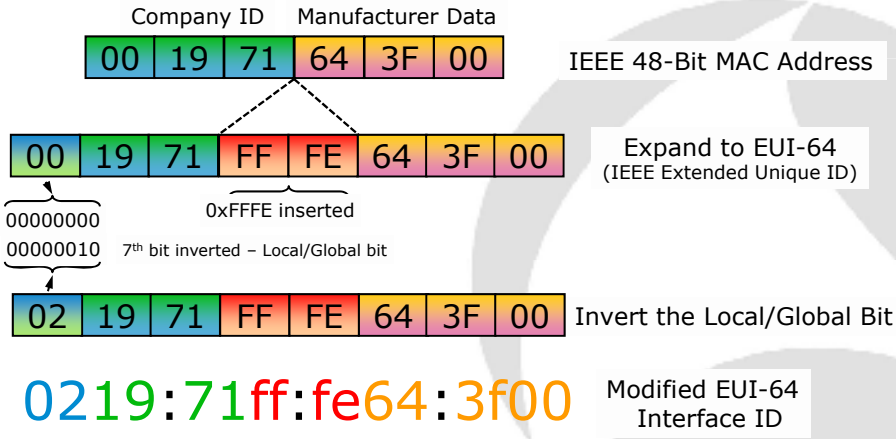
Address Scope	IPv4	IPv6
Link-Local - Not routable	Yes (is temp, APIPA)	Yes
Global Unicast - Routable to Internet	Aka public	Yes
Unique Local - Routable only within domain	Aka private RFC 1918	RFC 4193

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

13

Interface ID from MAC address

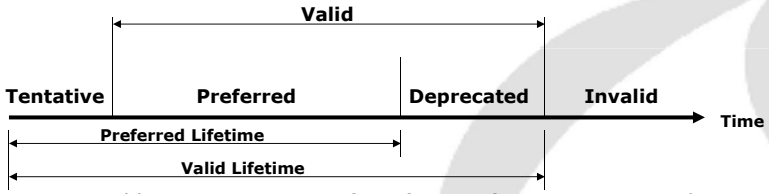


14

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

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

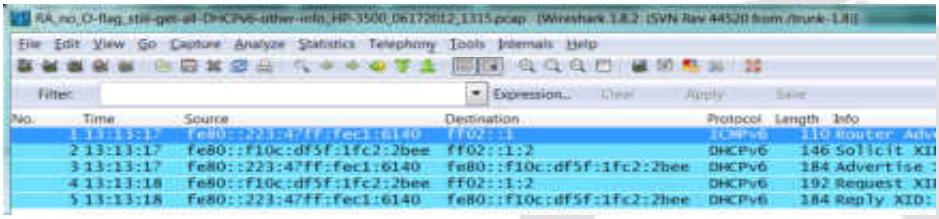
NDP ICMPv6 message types

- 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 M Flag	O Flag	ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info A Flag	L Flag	Prefix Derived from	Interface ID Derived from	Other Configuration Options	# of IPv6 Addr
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



- 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 and DNS

- Bind forward and reverse resolution

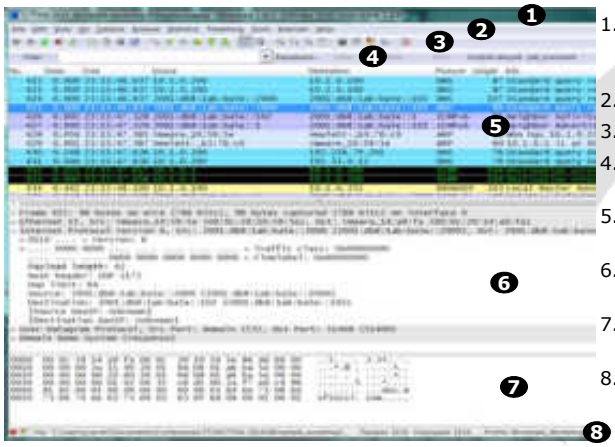
; 4to6labs.com Dumped
<snip>
www.4to6labs.com. 3600 IN AAAA 2607:f2f8:a6d0:0:0:0:0:2

; 0.0.0.0.0.d.6.a.8.f.2.f.7.0.6.2.ip6.arpa Dumped ;
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.6.a.8.f.2.f.7.0.6.2.ip6.arpa.
86400 IN PTR www.4to6labs.com.

Wireshark

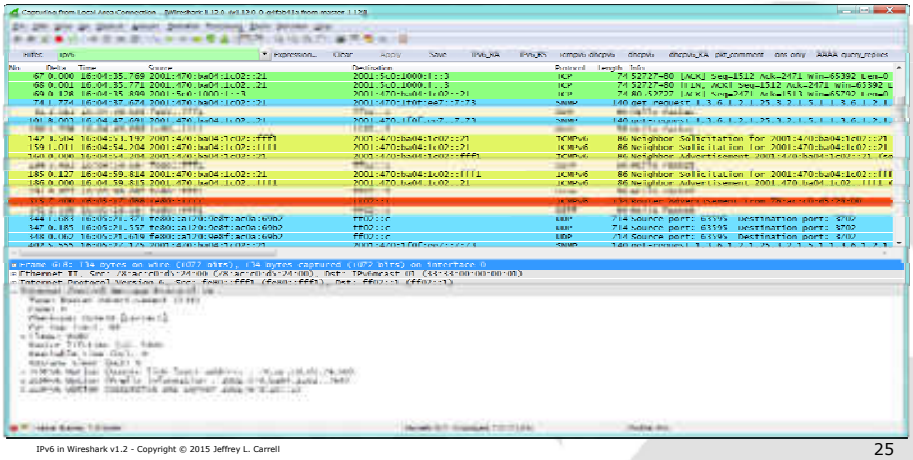
- Wireshark basics
- Wireshark color rules, display filters, columns and configuration profiles

Wireshark main view

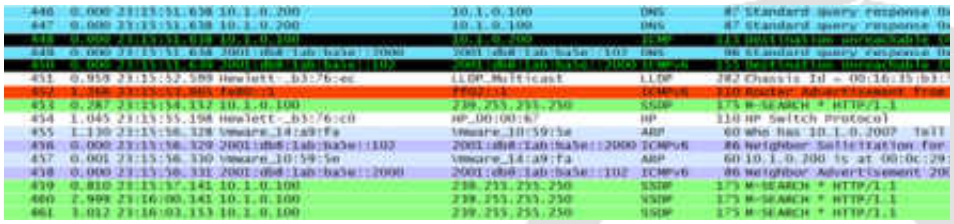


1. Title bar — trace file name or capture device name, and Wireshark version number
2. Main menu — standard menu
3. Main toolbar — quick access
4. Display filter area — reduce the amount of traffic you see
5. Packet List pane — summary of each frame
6. Packet Details pane — dissected frames
7. Packet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

Jeff's IPv6 Wireshark

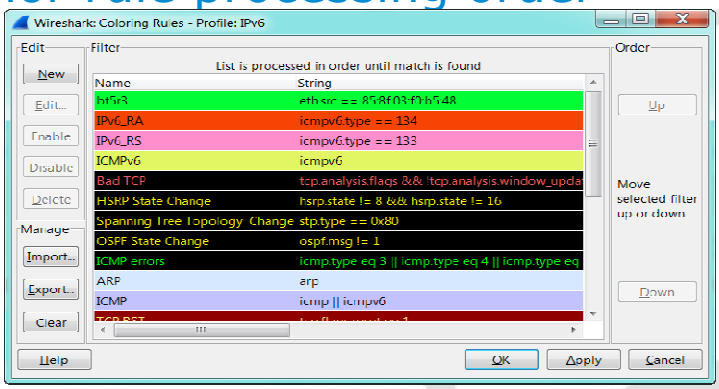


Coloring rules



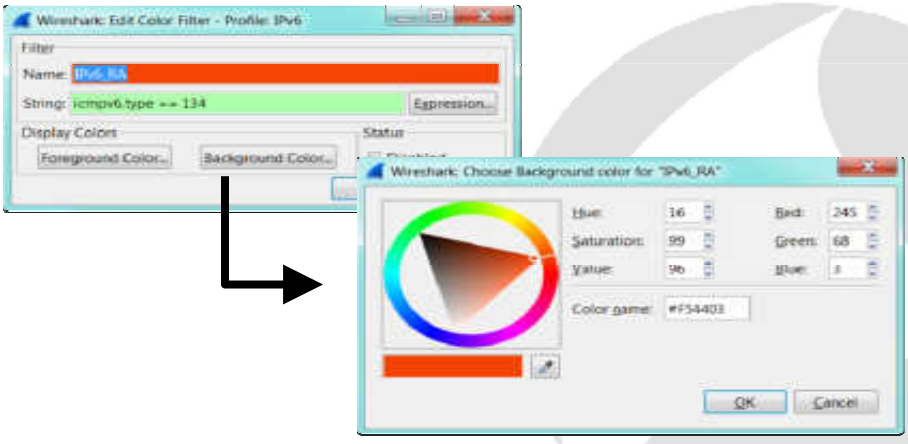
- Colors help you focus on specific address, protocols, events, and possibly find errors quickly

Color rule processing order

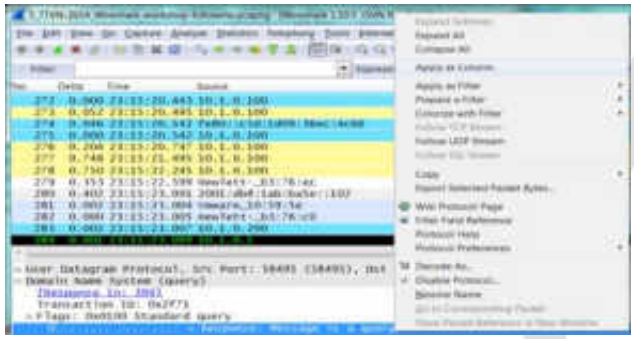


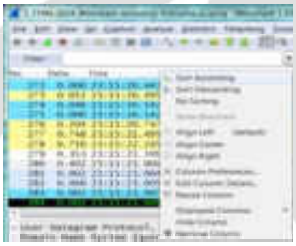
- Color rules read like a router ACL or firewall rule
  - First color rule that matches wins

Color rule creation



Columns

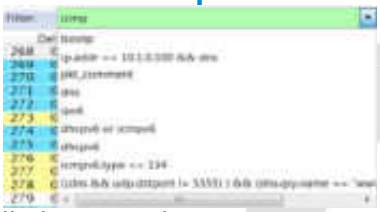




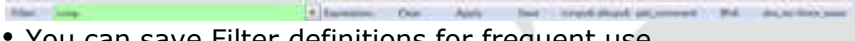
- In the Packet Details view, right-click on a specific field to Apply as Column
- Right-click column headings to sort, rename, align, etc

29

Display filters – option 1



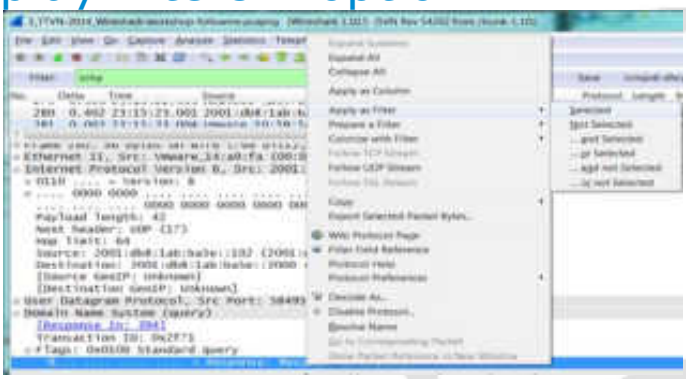
- The Filter bar will change colors as you type to signify correct syntax for the filter
  - Green – syntax is correct
  - Red – syntax is incorrect
  - Yellow – syntax is suspect
- The Filter dropdown will show last 10 filters used



- You can save Filter definitions for frequent use

30

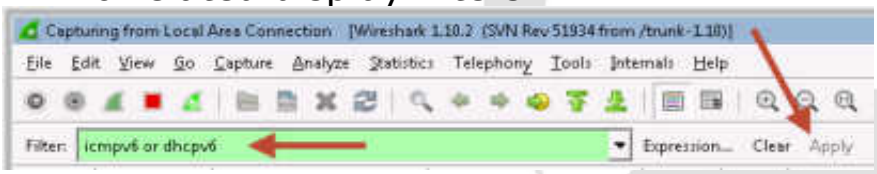
Display filters – option 2



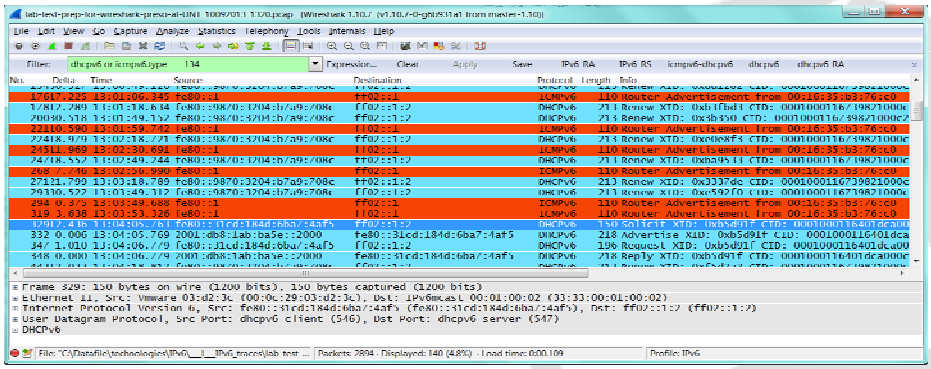
- In the Packet Details view, right-click on a specific field to build a filter

Using Wireshark to view IPv6 pkts

- IPv6 display filter families
  - ipv6
  - icmpv6
  - dhcpv6
- IPv6 related display filters:

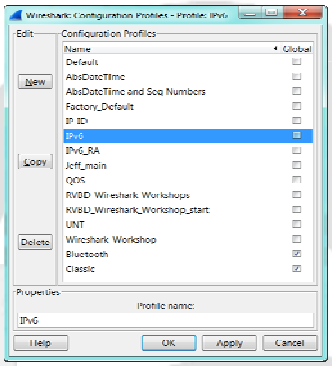


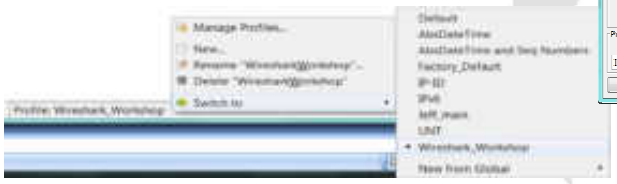
Using Wireshark to view IPv6 pkts



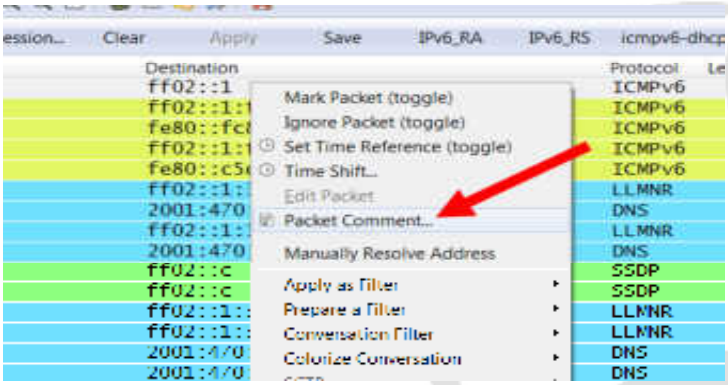
Configuration profiles

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





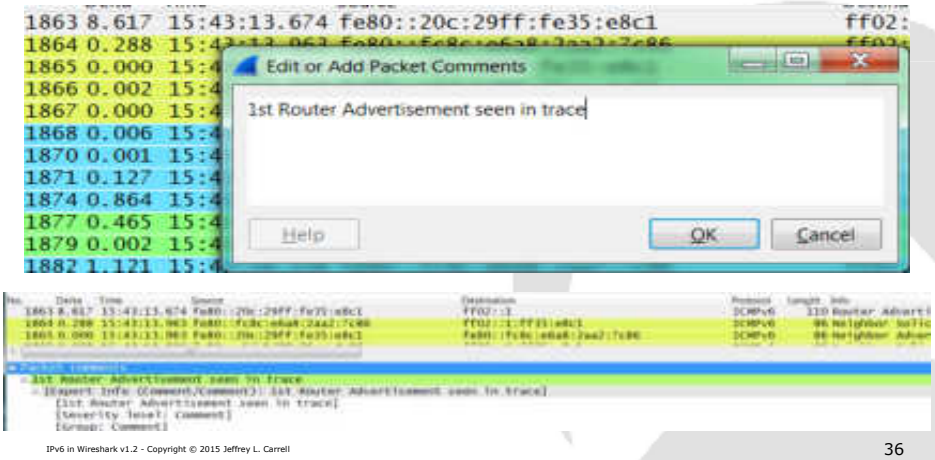
Packet annotation



- Right click packet, select Packet Comment

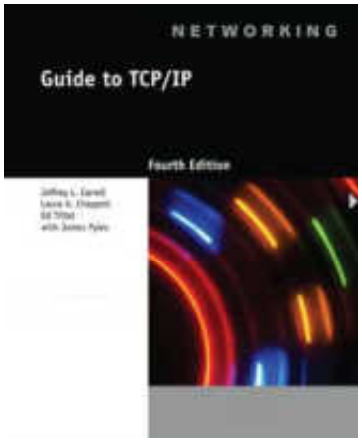
35

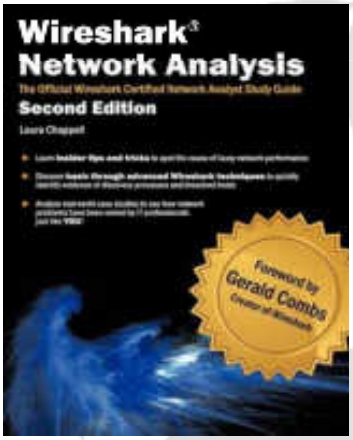
Packet annotation



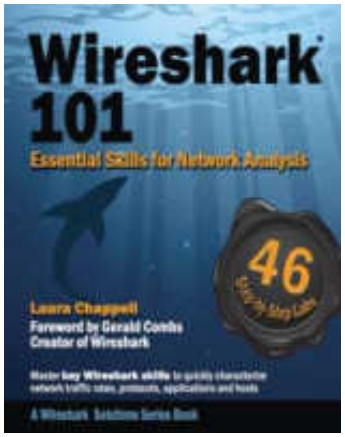
36

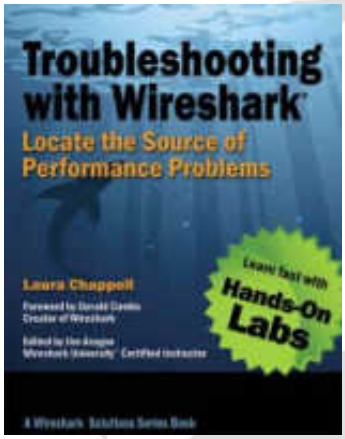
Resources



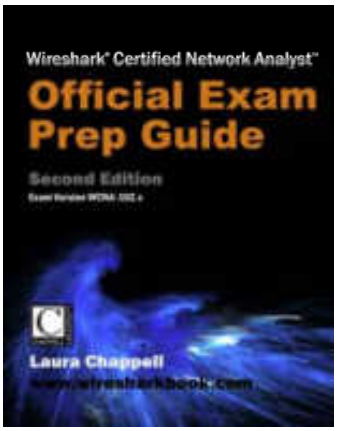


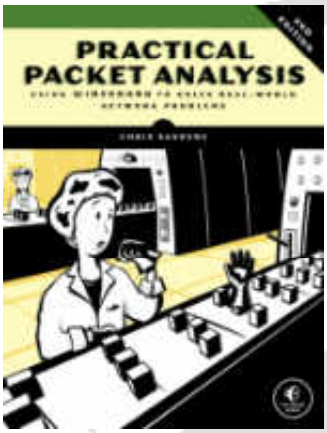
Resources



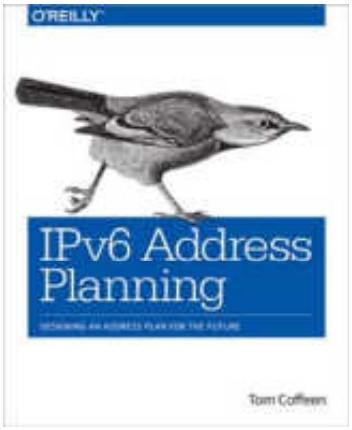


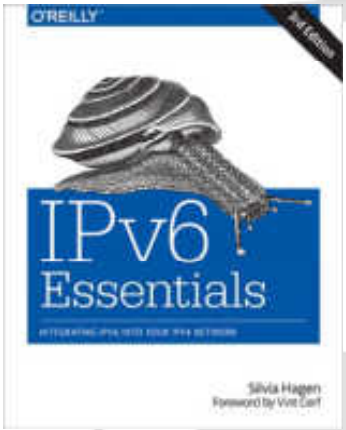
Resources



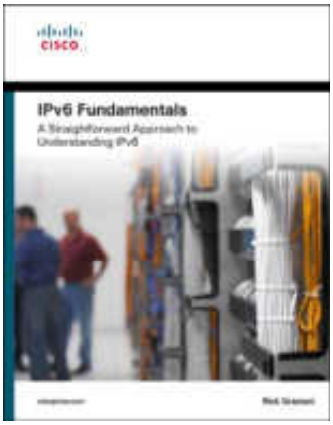


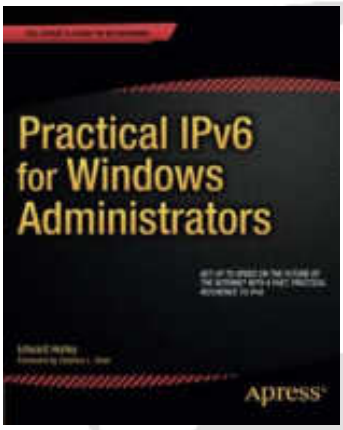
Resources





Resources





Thank You for Attending!

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