

IPv6 in Wireshark



IPv6 in Wireshark

Jeffrey L Carrell
Network Conversions
Network Consultant
IPv6 SME/Trainer
jeff.carrell@teachmeipv6.com
Twitter: @JeffCarrell_v6



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

1



IPv6 in Wireshark

- IPv6 – a bit more than basics
- Wireshark basics
- Wireshark color rules, display filters, columns and configuration profiles
- IPv6 in Wireshark

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

2

IPv6 in Wireshark



IPv6 – a bit more than basics

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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

3



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)

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

4

IPv6 in Wireshark



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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

5



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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

6

IPv6 in Wireshark



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
- $2001:0db8:1010:61ab:f005:ba11:00da:11a5/64$

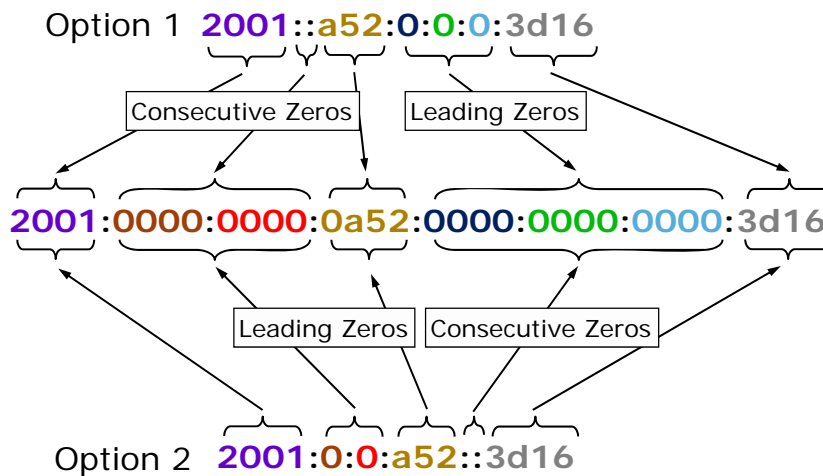
64bits for Network Identifier 64bits for Interface Identifier Prefix Length
- A single /64 network yields 18 billion-billion possible addresses

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

7




IPv6 shorthand notation



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

8

IPv6 in Wireshark



Incorrect shorthand notation


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

Consecutive Zeros Consecutive Zeros
Leading Zeros

2001::a52::3d16

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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 9



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 v1.2 - Copyright © 2015 Jeffrey L. Carrell 10

IPv6 in Wireshark



Address scopes

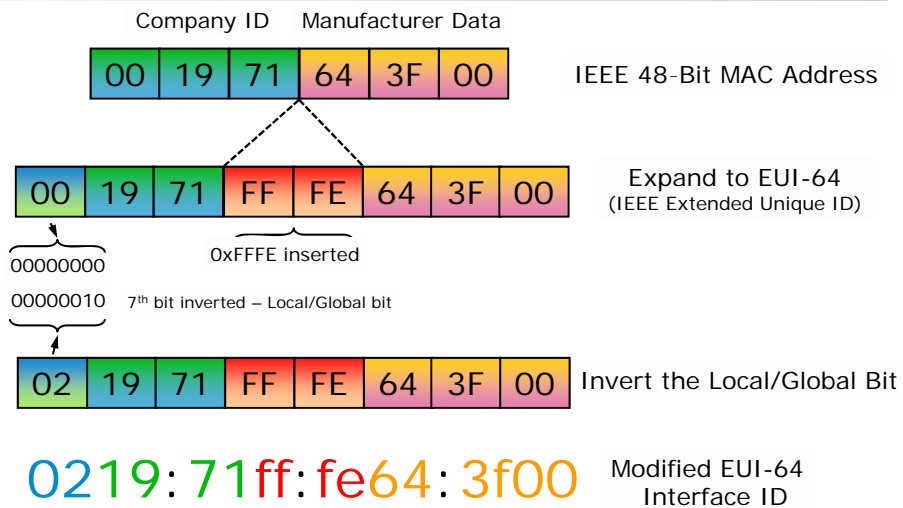
Address Scope	IPv4	IPv6
Link-Local - Not routable	Yes (is temp, APIPA)	Yes
Global Unicast - Routable to Internet	Aka public	Yes
Unique Local - Routable only within domain	Aka private RFC 1918	RFC 4193

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

11



Interface ID from MAC address



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

12

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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

13



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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

14

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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

15

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 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

16

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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

17




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)

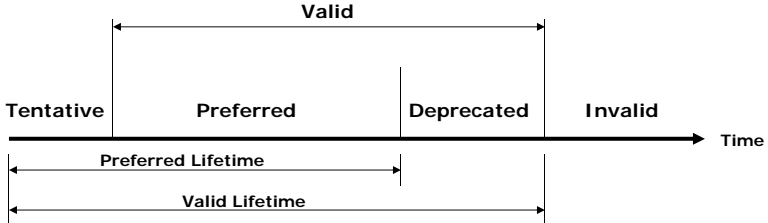
IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

18

IPv6 in Wireshark



Lifetime states of an IPv6 address




The diagram illustrates the lifecycle of an IPv6 address over time. It is divided into four states: Tentative, Preferred, Deprecated, and Invalid. A 'Valid' period encompasses the Preferred and Deprecated states. Two lifetimes are shown: 'Preferred Lifetime' which ends at the start of the Deprecated state, and 'Valid Lifetime' which ends at the start of the Invalid state.

- 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

19




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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

20


IPv6 in Wireshark



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 v1.2 - Copyright © 2015 Jeffrey L. Carrell 21



IPv6 address autoconfiguration

- Assigning an IPv6 address:
 - **Link-Local** (automatically assigned when IPv6 is enabled)
 - Based on prefix fe80::/10, assigned as fe80::/64
 - Interface ID (64 bit host portion) derived from either:
 - Modified IEEE EUI-64 format (RFC 4291)
 - Derived from MAC address
 - Privacy format (RFC 4941)
 - Derived from random number generator

❖ **NOTE:** Requires no routers, no DHCPv6 servers, no additional network systems support

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 22

IPv6 in Wireshark



Link-Local address basics

- Each interface must have one (and only one) link-local address (generally autoconfigured by OS)
- Can/may be same on any/all interfaces
- Zone ID or Scope ID is used to differentiate which interface is to be used for outbound communications
- Zone ID is appended to link-local address when used for outbound communications

ping fe80::22c:8a5c:12ab:370f%vlan1 - switch

ping fe80::22c:8a5c:12ab:370f%12 - Windows

ping fe80::22c:8a5c:12ab:370f%eth0 - Linux

^destination host to ping ^intf to go out

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

23



Link-Local address status (Win7)

Windows 7 example:

```
C:\>ipconfig /all |more
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : example.com
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 00-9C-02-8F-61-F4
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a120:9e8f:ac0a:69b2%12(Preferred)
IPv4 Address. . . . . : 10.1.1.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

```
C:\>netsh int ipv6 show address interface=12
```

```
Address fe80::a120:9e8f:ac0a:69b2%12 Parameters
```

```
-----
Interface Luid      : Local Area Connection
Scope Id           : 0.12
Valid Lifetime    : infinite
Preferred Lifetime : infinite
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

24

IPv6 in Wireshark



Link-Local neighbors (Win7)

- Windows 7 example:

```
C:\>netsh int ipv6 show neighbors interface=12
```

Interface 12: Local Area Connection

Internet Address	Physical Address	Type
2001:470:1f0f:ee7::1	00-09-0f-db-04-d3	Stale (Router)
fe80::209:fff:fedb:4d3	00-09-0f-db-04-d3	Stale (Router)
ff02::1	33-33-00-00-00-01	Permanent
ff02::2	33-33-00-00-00-02	Permanent
ff02::c	33-33-00-00-00-0c	Permanent
ff02::16	33-33-00-00-00-16	Permanent
ff02::fb	33-33-00-00-00-fb	Permanent
ff02::1:2	33-33-00-01-00-02	Permanent
ff02::1:3	33-33-00-01-00-03	Permanent
ff02::1:ff00:1	33-33-ff-00-00-01	Permanent
ff02::1:ff07:101	33-33-ff-07-01-01	Permanent
ff02::1:ff0a:69b2	33-33-ff-0a-69-b2	Permanent
ff02::1:ff15:d7a3	33-33-ff-15-d7-a3	Permanent
ff02::1:ffdb:4d3	33-33-ff-db-04-d3	Permanent

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

25



Link-Local usage (Win7)

- Windows 7 example:

```
C:\>ping fe80::209:fff:fedb:4d3%12
```

Pinging fe80::209:fff:fedb:4d3%12 with 32 bytes of data:

```
Reply from fe80::209:fff:fedb:4d3%12: time<1ms
```

```
Reply from fe80::209:fff:fedb:4d3%12: time<1ms
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

26

IPv6 in Wireshark



Link-Local address status (Mac)

- Mac OS X 10.9.1 example:

```
mac: ~ jcarrell$ ifconfig -L en0
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu
1500
options=27<RXCSUM, TXCSUM, VLAN_MTU, TSO4>
ether 00:23:32:c9:f3:c4
inet6 fe80::223:32ff:fec9:f3c4%en0 prefixlen 64 scopeid 0x4
inet 192.168.1.199 netmask 0xfffff00 broadcast 192.168.1.255
inet6 2001:5c0:1506:ef00::119 prefixlen 64 pltime 138 vltime 251
nd6 options=1<PERFORMNUD>
media: autoselect (100baseTX <full-duplex,flow-control>)
status: active
```



Link-Local neighbors (Mac)

- Mac OS X 10.9.1 example:

```
mac:~ jcarrell1$ ndp -an - show IPv6 neighbors
Neighbor                Linklayer Address  Netif  Expire    St Flgs Prbs
2001:5c0:1506:ef00::119  0:23:32:c9:f3:c4  en0    permanent R
fe80::1%lo0              (incomplete)      lo0    permanent R
fe80::223:32ff:fec9:f3c4%en0  0:23:32:c9:f3:c4  en0    permanent R
fe80::a00:27ff:fe3f:556e%en0  8:0:27:3f:55:6e   en0    2s       R  R
```

IPv6 in Wireshark



Link-Local usage (Mac)

- Mac OS X 10.9.1 example:

```
mac:~ jcarrell$ ping6 fe80::a00:27ff:fe3f:556e%en0
PING6(56=40+8+8 bytes) fe80::223:32ff:fec9:f3c4%en0 -->
  fe80::a00:27ff:fe3f:556e%en0
16 bytes from fe80::a00:27ff:fe3f:556e%en0, icmp_seq=0 hlim=64 time=0.366 ms
16 bytes from fe80::a00:27ff:fe3f:556e%en0, icmp_seq=1 hlim=64 time=0.630 ms
^C
--- fe80::a00:27ff:fe3f:556e%en0 ping6 statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.366/0.498/0.630/0.120 ms

mac:~ jcarrell$ ping6 fe80::a00:27ff:fe3f:556e
PING6(56=40+8+8 bytes) fe80::223:32ff:fec9:f3c4%en0 -->
  fe80::a00:27ff:fe3f:556e
ping6: sendmsg: No route to host
ping6: wrote fe80::a00:27ff:fe3f:556e 16 chars, ret=-1
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

29



Link-Local address status (HP)

- HP ProVison Layer3 switch example:

```
HP3500# show ipv6

Internet (IPv6) Service

IPv6 Routing      : Enabled
ND DAD           : Enabled
DAD Attempts     : 3

                                VLAN Interfaces
Interface Name   : v12-client-vlan
IPv6 Status      : Enabled
Layer 3 Status   : Enabled

Address          |                               Address
Origin           | IPv6 Address/Prefix Length    | Status
-----+-----
manual          | 2001:470:c9:1692::f254/64     | preferred
manual          | fe80::9/64                    | preferred
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

30

IPv6 in Wireshark



Link-Local usage (HP)

- HP ProVision Layer3 switch example:

```
HP3500# show ipv6 neighbors
```

```
IPv6 ND Cache Entries
IPv6 Address                               MAC Address  State Type  Port
-----
fe80::2cab:3680:143d:603a%vlan2          000c29-34478a STALE dynamic 8
2001:470:56:1ff9::1                       4001c6-a6aa81 REACH dynamic 1
```

```
HP3500# ping6 fe80::2cab:3680:143d:603a%vlan2
fe80::2cab:3680:143d:603a is alive, time = 5 ms
```

```
HP3500# ping6 fe80::2cab:3680:143d:603a [I did not supply vlan-id,
I simply pressed <ENTER>]
Specified address must include an interface scope. For example, to specify
the link-local address "fe80::1" on VLAN 1, use: fe80::1%vlan1.
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

31



Link-Local address status (Cisco)

- Cisco Layer3 switch example:

```
Cisco3750#show ipv6 interface vlan 2
Vlan2 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::5
Global unicast address(es):
  2001:470:56:1652::F254, subnet is 2001:470:56:1652::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::5
  FF02::6
  FF02::1:2
  FF02::1:FF00:5
  FF02::1:FF00:F254
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

32

IPv6 in Wireshark



Link-Local usage (Cisco)

- Cisco Layer3 switch example:

```
Cisco3750#show ipv6 neighbors
```

```
IPv6 Address                               Age Link-layer Addr State Interface
FE80::250E:BB04:9D92:370E                 0 000c.2997.60e8 STALE V12
2001:470:56:1652::102                     1 000c.2997.60e8 STALE V12
FE80::F254                                 0 4001.c6a6.aa81 STALE V11
```

```
Cisco3750#ping ipv6 fe80::250e:bb04:9d92:370e
```

```
Output Interface: vlan 2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to FE80::250E:BB04:9D92:370E, timeout is 2 seconds:
```

```
Packet sent with a source address of FE80::5
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
Cisco3750#ping ipv6 fe80::250e:bb04:9d92:370e
```

```
Output Interface: [I did not supply vlan-id, I simply pressed <ENTER>]
```

```
% Interface required
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

33



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 (DNS, domain, time, ftp, etc) Derived via	# 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

34

IPv6 in Wireshark



IPv6 address autoconfiguration

- Assigning an IPv6 address:
 - **SLAAC** (Stateless address autoconfiguration), generally a /64
 - Uses prefix information from Router Advertisement
 - Interface ID (64 bit host portion) derived from either:
 - Modified IEEE EUI-64 format (RFC 4291)
 - Derived from MAC address
 - Privacy format (RFC 4941)
 - Derived from random number generator
 - Generally creates 2 global addresses
 - Cryptographically generated (RFC 3971 & 3972)
 - Secure/unique interface ID

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

35



IPv6 SLAAC process

- A node sends a multicast Router Solicitation message to the “all-routers” address ff02::2
- Router(s) respond with Router Advertisement message containing A & L flags “on” and prefix(es) for stateless autoconfiguration
- The node configures its own IPv6 address(es) with the advertised prefix(es), plus a locally-generated Interface ID
- Node checks whether the selected address(es) is(are) unique (Duplicate Address Detection)
- If unique, the address(es) is(are) configured on interface
- **Note – no DNS automatically configured**

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

36

IPv6 in Wireshark



ICMPv6 - Router Advertisement

- Router Advertisement (RA) [key components]
 - M flag – managed address configuration flag (for stateful (DHCPv6) autoconfig)
 - O flag – other configuration flag (for stateless DHCPv6 autoconfig)
 - Prf flag – router preference flag (ska priority)
 - Router Lifetime – lifetime associated with the default router
 - Prefix Length – number of bits in the prefix
 - **A flag – autonomous address-configuration flag** (for SLAAC)
 - **L flag – on-link flag**
 - Valid Lifetime – length of time the address is valid for use in preferred and deprecated states
 - Preferred Lifetime – length of time the address is valid for new communications
 - Prefix – IPv6 address prefix

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

– For additional info, see RFC 4861

37






Router Advertisement packet (Stateless)

```
No.    Delta Time      Source                Destination           Protocol Length Info
-----
267/ 32.815 14:38:24.440 fe80::21b:3fff:feb:1d00 ff02::1               ICMPv6 110 Router Advertisement
    [ethernet II]
    [Frame 267: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface]
    [Ethernet II, Src: ProCurve-0b:1d:00:00:1b:3f:db:1d:00, Dst: IPv6mcast-00:00:00:01:33:33:00:00:01]
    [Internet Protocol Version 6, Src: fe80::21b:3fff:feb:1d00 (fe80::21b:3fff:feb:1d00), Dst: ff02::1 (ff02::1)]
    [Internet Control Message Protocol v6]
      Type: Router Advertisement (134)
      Code: 0
      Checksum: 0x5293 [correct]
      Cur_hop_limit: 64
    [Flags: 0x00]
      0... .. = Managed address configuration: Not set
      .0... .. = Other configuration: Not set
      ..0... .. = Home Agent: Not set
      ...0... .. = Prf (Default Router Preference): Medium (0)
      ....0... .. = Proxy: Not set
      .....0... .. = Reserved: 0
      Router lifetime (s): 0
      Reachable time (ms): 0
      Retrans timer (ms): 0
    [ICMPv6 Option (Source link-layer address : 00:1b:3f:db:1d:00)]
    [ICMPv6 Option (Prefix information : 2001:db8:1ab:ba5e::/64)]
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    [Flag: 0xc0]
      1... .. = On-link flag(L): Set
      .1... .. = Autonomous address-configuration flag(A): Set
      ..0... .. = Router address flag(R): Not set
      ...00000 = Reserved: 0
      Valid Lifetime: 0
      Preferred Lifetime: 0
      Reserved
      Prefix: 2001:db8:1ab:ba5e:: (2001:db8:1ab:ba5e::)
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

38




IPv6 in Wireshark

IPv6 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options (DNS, domain, time, tftp, etc) Derived via	# 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell 39

- 


- ## IPv6 address autoconfiguration
- Assigning an IPv6 address:
 - **Stateful** (DHCPv6), generally a /64
 - DHCPv6 (RFC 3315)
 - Uses prefix information defined in scope
 - Interface ID (64 bit host portion) derived from scope pool
 - Reply includes “other” information
 - DNS, domain, time server, tftp or download server, etc
- IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 40

IPv6 in Wireshark



IPv6 Stateful (DHCPv6) process

- A node sends a multicast Router Solicitation message to the “all-routers” address ff02::2
- Router(s) respond with Router Advertisement message containing M flag for stateful autoconfiguration
- The node sends a multicast Solicit message to the “all-DHCP relay agents and servers” address ff02::1:2
- DHCPv6 server(s) responds with Advertise message(s) containing IPv6 address and lifetimes
- The node sends a Request message to confirm and seeking other information
- DHCPv6 server responds with Reply message
- Node checks whether the selected address is unique (Duplicate Address Detection)
- If unique, the address is configured on interface

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

41



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 XII
5	13:13:18	fe80::223:47ff:fec1:6140	fe80::f10c:df5f:1fc2:2bee	DHCPv6	184	Reply XIX:

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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

42

IPv6 in Wireshark



ICMPv6 - Router Advertisement

- Router Advertisement (RA) [key components]
 - **M flag – managed address configuration flag**
(for stateful (DHCPv6) autoconfig)
 - **O flag – other configuration flag**
(for stateless DHCPv6 autoconfig)
 - Prf flag – router preference flag (ska priority)
 - Router Lifetime – lifetime associated with the default router
 - Prefix Length – number of bits in the prefix
 - **A flag – autonomous address-configuration flag** (for SLAAC)
 - **L flag – on-link flag**
 - Valid Lifetime – length of time the address is valid for use in preferred and deprecated states
 - Preferred Lifetime – length of time the address is valid for new communications
 - Prefix – IPv6 address prefix

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

– For additional info, see RFC 4861

43



Router Advertisement packet (Stateful/DHCPv6)

```
No.    Time    Source                               Destination    Protocol Length Info
-----
1782  12.18:21  fe80::20c:29ff:fe35:e8c1            ff02::1       ICMPv6      110  Router Advertisement
<----->
Frame 1282: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: Vmware_35:e8:c1 (00:0c:29:35:e8:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::20c:29ff:fe35:e8c1 (fe80::20c:29ff:fe35:e8c1), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xe3c1 [correct]
  Cur_hop limit: 64
  Flags: 0xc0
    1... .. = Managed address configuration: Set
    .1... .. = Other configuration: Set
    ..0... .. = Home Agent: Not set
    ...0 0... = Prf (Default Router Preference): Medium (0)
    ....0... = Proxy: Not set
    .... ..0 = Reserved: 0
  Router lifetime (s): 540
  Reachable time (ms): 0
  Retrans timer (ms): 0
  ICMPv6 Option (Prefix information : 2001:db8:1ab:ba5e::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
  Flag: 0x80
    1... .. = On-link flag(L): Set
    ..0... .. = Autonomous address-configuration flag(A): Not set
    ...0... .. = Router address flag(R): Not set
    ...0 0000 = Reserved: 0
  Valid Lifetime: 300
  Preferred Lifetime: 240
  Reserved
  Prefix: 2001:db8:1ab:ba5e:: (2001:db8:1ab:ba5e::)
  ICMPv6 Option (Source link-layer address : 00:0c:29:35:e8:c1)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: Vmware_35:e8:c1 (00:0c:29:35:e8:c1)
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

44

IPv6 in Wireshark



Key difference in DHCP/DHCPv6

- Default gateway
 - DHCP – configurable Router option in scope
 - DHCPv6 – no configurable Router option in scope (possible future, but no client OS support yet)
- An IPv6 node derives its default gateway from the router's Link-Local address when the L flag is set in the Prefix information field of an RA
(! not from the network prefix !)

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

45

W2K8-R2 DHCPv6 server operation



Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID
2001:db8:1ab:ba5e::102	Win7_02.ipv6sando...	Reservation (active)	234884137	IANA	00010001163f0053000c29418d2d
2001:db8:1ab:ba5e::105		5/31/2013 8:17:22 AM	0	IANA	000100011696877dc8bcc8a01693
2001:db8:1ab:ba5e::109	Win7_03.ipv6sando...	Reservation (inactive)	234884137	IANA	00010001180f12e5000c29e88b3d

Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID
2001:db8:1ab:ba5e::102	Win7_02.ipv6sando...	Reservation (active)	234884137	IANA	00010001163f0053000c29418d2d

```
Internet Protocol Version 6, Src: 2001:db8:1ab:ba5e::2000 (2001:db8:1ab:ba5e::2000),
User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)
DHCPv6
  Message type: Reply (7)
  Transaction ID: 0xb3670f
  Server identifier: 000100004ee1d205000c29a14a20
  Client identifier: 00010001163f0053000c29418d2d
  Identity Association for Non-temporary Address
    Option: Identity Association for Non-temporary Address (3)
      Length: 40
      Value: 0e000c2900000f0000001800005001820010db801abba5e...
      IAID: 0e000c29
      T1: 240
      T2: 384
  TA Address: 2001:db8:1ab:ba5e::102
  Domain Search List
    Option: Domain Search List (24)
      Length: 17
      Value: 0b6970763672616e64626f7803636f6d00
      DNS Domain Search List
        Domain: ipv6sandbox.com
  DNS recursive name server
    Option: DNS recursive name server (23)
      Length: 16
      Value: 20010db801abba5e0000000000002000
      DNS servers address: 2001:db8:1ab:ba5e::2000
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

46

IPv6 in Wireshark



DHCPv6 Unique Identifier - DUID

- Each DHCPv6 client and server has a DUID
- DHCPv6 servers use DUIDs to identify clients for the selection of configuration parameters and in the association of IAs with clients
- DHCPv6 clients use DUIDs to identify a server in messages where a server needs to be identified

(ref RFC 3315)

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

47



Cloning clients and DUID

- When a client machine is cloned, all the clones have the same DUID
- When 2 clients with the same DUID request an IPv6 address, the DHCPv6 server provides the same address to both clients
- When the 2nd client performs DAD, it detects an IPv6 address conflict, and will not go "on link"

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

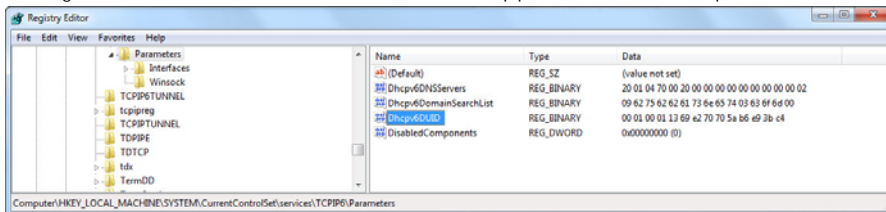
48

IPv6 in Wireshark



Cloning clients and DUID

- For cloned Microsoft Windows clients, the DUID is in the Windows Registry and can be removed with a manual operation (regedit)
- This should be done before creating a clone, so that when the clones clients are booted, new and unique DUIDs will be created
- reg delete HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters /f /v Dhcpv6DUID



49

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 (DNS, domain, time, ftp, etc) Derived via	# 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

50

IPv6 in Wireshark



IPv6 address autoconfiguration

- Assigning an IPv6 address:
 - **Stateless DHCPv6**
 - Uses prefix information from Router Advertisement
 - Interface ID (64 bit host portion) derived from either:
 - Modified IEEE EUI-64 format (RFC 4291)
 - Derived from MAC address
 - Privacy format (RFC 4941)
 - Derived from random number generator
 - Cryptographically generated (RFC 3971 & 3972)
 - Secure/unique interface ID
 - Uses DHCPv6 for “other” information
 - DNS, domain, time server, tftp or download server, etc

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

51



IPv6 Stateless DHCPv6 process

- A node sends a multicast Router Solicitation message to the “all-routers” address ff02::2
- Router(s) respond with Router Advertisement message containing A & L flags “on” and prefix(es), and O flag “on” for stateless DHCPv6 autoconfiguration
- The node configures its own IPv6 address(es) with the advertised prefix(es), plus a locally-generated Interface ID
- The node sends a multicast Information-Request message to the “all-DHCP relay agents and servers” address ff02::1:2
- DHCPv6 server responds with Reply message
- Node checks whether the selected address is unique (Duplicate Address Detection)
- If unique, the address is configured on interface

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

52

IPv6 in Wireshark



ICMPv6 - Router Advertisement

- Router Advertisement (RA) [key components]
 - M flag – managed address configuration flag (for stateful (DHCPv6) autoconfig)
 - **O flag – other configuration flag** (for stateless DHCPv6 autoconfig)
 - Prf flag – router preference flag (ska priority)
 - Router Lifetime – lifetime associated with the default router
 - Prefix Length – number of bits in the prefix
 - **A flag – autonomous address-configuration flag** (for SLAAC)
 - **L flag – on-link flag**
 - Valid Lifetime – length of time the address is valid for use in preferred and deprecated states
 - Preferred Lifetime – length of time the address is valid for new communications
 - Prefix – IPv6 address prefix

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

– For additional info, see RFC 4861

53



Router Advertisement packet (Stateless/DHCPv6)

```
6000 5.346 09:33:22.152 fe80::2 ff02::1 ICMPv6 118 Router Advertisement
<----->
| Ethernet II, Src: Cisco_54:4b:c0 (00:11:21:54:4b:c0), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01) |
| Internet Protocol Version 6, Src: fe80::2 (fe80::2), Dst: ff02::1 (ff02::1) |
| Internet Control Message Protocol v6 |
| Type: Router Advertisement (134) |
| Code: 0 |
| Checksum: 0x8df9 [correct] |
| Cur_hop_limit: 64 |
| Flags: 0x40 |
| 0... .. = Managed address configuration: Not set |
| .1... .. = Other configuration: Set |
| ..0... .. = Home Agent: Not set |
| ...0... = Prf (Default Router Preference): Medium (0) |
| ....0.. = Proxy: Not set |
| .....0. = Reserved: 0 |
| Router Lifetime (s): 1800 |
| Reachable time (ms): 0 |
| Retrans timer (ms): 0 |
| ICMPv6 Option (Source link-layer address : 00:11:21:54:4b:c0) |
| ICMPv6 Option (MTU : 1500) |
| ICMPv6 Option (Prefix information : 2001:db8:1ab:ba5e::/64) |
| Type: Prefix information (3) |
| Length: 4 (32 bytes) |
| Prefix Length: 64 |
| Flag: 0xc0 |
| 1... .. = On-link flag(L): Set |
| .1... .. = Autonomous address-configuration flag(A): Set |
| ..0... .. = Router address Flag(R): Not set |
| ...0000 = Reserved: 0 |
| Valid Lifetime: 35 |
| Preferred Lifetime: 15 |
| Reserved |
| Prefix: 2001:db8:1ab:ba5e:: (2001:db8:1ab:ba5e::) |
```

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

54

IPv6 in Wireshark



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 (DNS, domain, time, ftp, etc) Derived via	# 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

55






Combination Stateless and DHCPv6

- This is typically an undesired configuration
- Generally a result of enabling RA flags for one type of address autoconfiguration requirement, and not disabling other flags not required
- Result is too many/unwanted IPv6 GUA's
 - SLAAC – up to two possible GUA's
 - Stateful (DHCPv6) – one GUA
 - Even a manual configured GUA
- ❖ Remember, if there is a “Temporary” GUA, it will be used for outbound communications

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

56




IPv6 in Wireshark


IPv6 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options (DNS, domain, time, tftp, etc) Derived via	# 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell 57

- 


- ## Manual configured IPv6 addresses
- In Windows operating systems (server and client), does not over-ride DHCPv6 functions (like it does in IPv4)
 - If don't want SLAAC or DHCPv6 addresses on network segment, must disable A, M, and O flags in RA
 - Do not need to configure default gateway, but can
 - Remember, how does an IPv6 node derive a router ???
 - May be able to manually configure Link-local address, handy for routers so configuration is "portable"
 - Generally not possible on client OSs
- IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 58

IPv6 in Wireshark



IPv6 notation in URL

IPv6 Characters URL Characters


https://[2001:0:0:a52::3d16]:5678/webpage.html

Enclose IPv6 Address in Square Brackets Optional Port ID

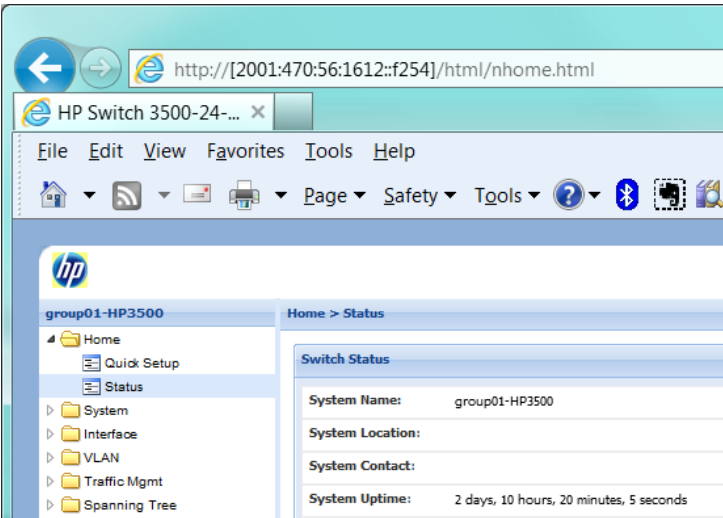
For additional info, see RFC 5952

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 59

Detailed description: This diagram illustrates the components of an IPv6 URL. The URL 'https://[2001:0:0:a52::3d16]:5678/webpage.html' is shown. Yellow arrows point from 'IPv6 Characters' to the IPv6 address '2001:0:0:a52::3d16'. Blue arrows point from 'URL Characters' to the 'https://', the port '5678', and the path '/webpage.html'. Green arrows point from 'Enclose IPv6 Address in Square Brackets' to the square brackets around the IPv6 address. A black arrow points from 'Optional Port ID' to the port number '5678'.



IPv6 GUA in URL



http://[2001:470:56:1612::f254]/html/nhome.html

HP Switch 3500-24-...

File Edit View Favorites Tools Help

HP logo

group01-HP3500

Home > Status

Switch Status

System Name: group01-HP3500

System Location:

System Contact:

System Uptime: 2 days, 10 hours, 20 minutes, 5 seconds

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 60

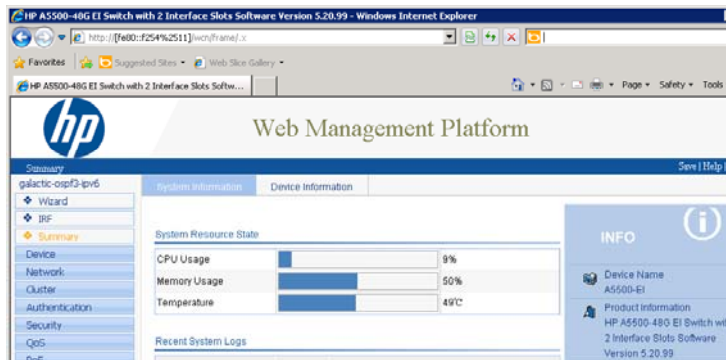
Detailed description: This is a screenshot of a web browser window. The address bar shows the URL 'http://[2001:470:56:1612::f254]/html/nhome.html'. The browser title is 'HP Switch 3500-24-...'. The browser interface includes a menu bar (File, Edit, View, Favorites, Tools, Help) and a toolbar with various icons. The main content area displays the HP logo and a navigation tree on the left with items like Home, Quick Setup, Status, System, Interface, VLAN, Traffic Mgmt, and Spanning Tree. On the right, there is a 'Home > Status' section with a 'Switch Status' table containing fields for System Name, System Location, System Contact, and System Uptime.

IPv6 in Wireshark



IPv6 Link-local in URL

- `http://[fe80::f254%2511]`
 - `fe80::f254` is destination, `%11` is the outbound interface – but specified as `%2511` where the `%25` is hex converted to the `%` symbol
 - ❖ Note, this does not work in all browsers

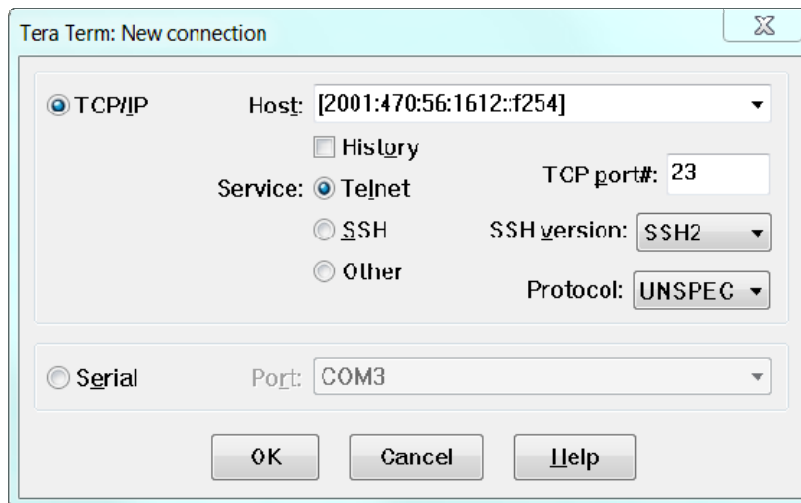


IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

61



Telnet/SSH over IPv6



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

62

IPv6 in Wireshark



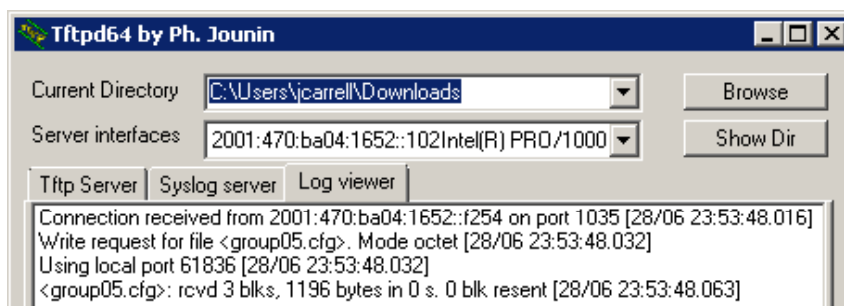
Telnet/SSH over IPv6

```
group05-NetIron#show telnet
Console connections:
    established, privilege super-user
    you are connecting to this session
    4 seconds in idle
Telnet server status: Enabled
Telnet connections (inbound):
  1    established, client ip6 address
2001:470:1f0f:ee7::7:100, privilege super-user
    using vrf default-vrf.
```

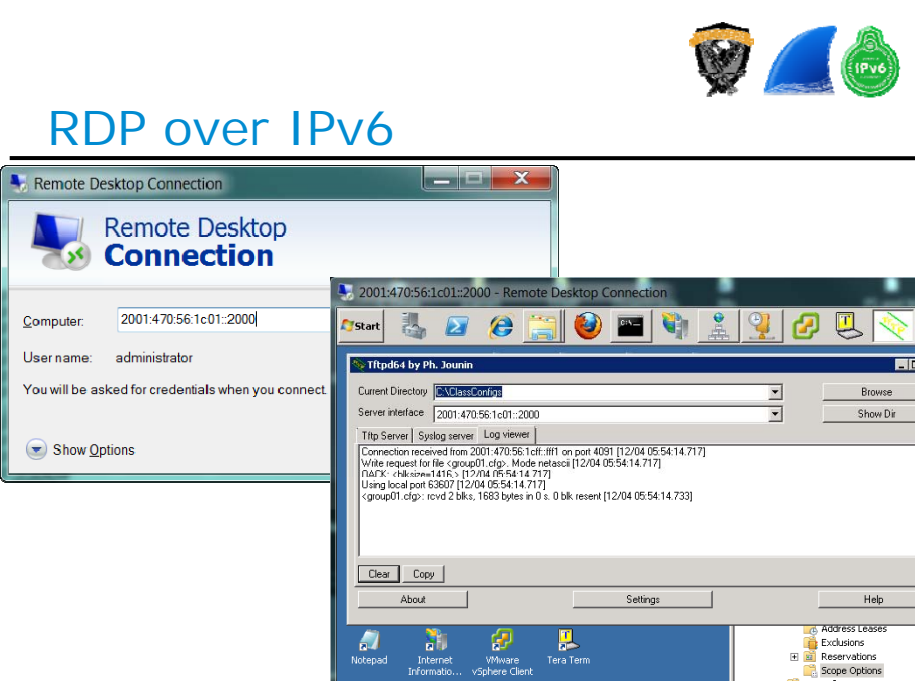


TFTP over IPv6

```
group05-NetIron#copy running-config tftp ipv6
2001:470:ba04:1652::102 group05.cfg
```



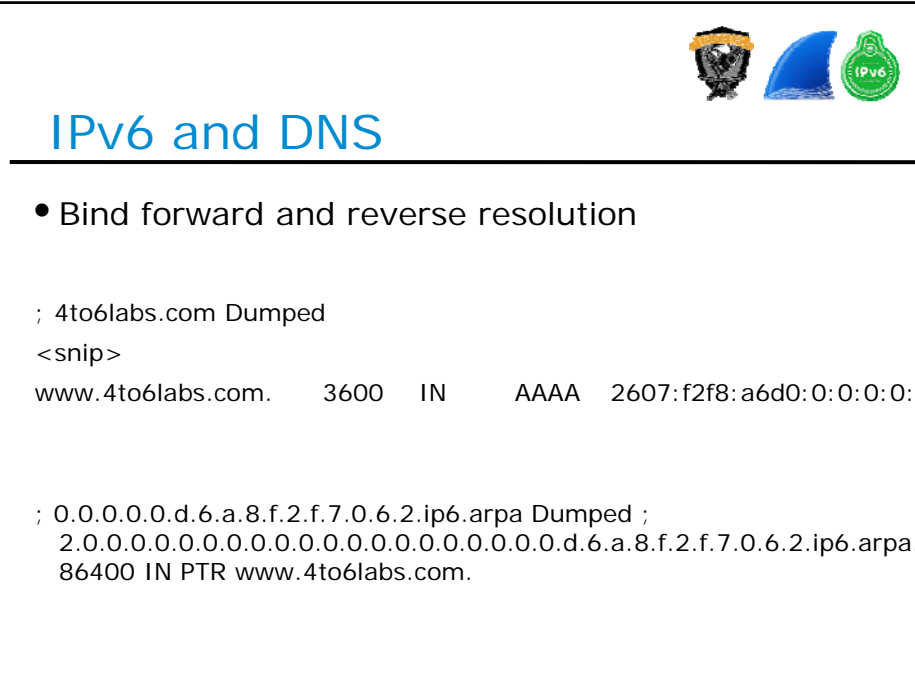
IPv6 in Wireshark



The screenshot shows a Windows Remote Desktop Connection window. The 'Computer' field is set to '2001:470:56:1c01::2000' and the 'User name' is 'administrator'. A second window titled '2001:470:56:1c01::2000 - Remote Desktop Connection' is open, displaying network traffic logs. The logs show a connection request from '2001:470:56:1c01::#11' on port 4091, a write request for a file, and a local port binding for 'group01.cdp'. The interface also shows 'Tftp Server', 'Syslog server', and 'Log viewer' tabs.

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

65



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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

66

IPv6 in Wireshark



Wireshark

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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

67

Wireshark main view




The screenshot shows the Wireshark main view interface. The top bar displays the file name and version. Below it is a menu bar and a toolbar. A filter bar is present above the packet list pane. The packet list pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 6, and User Datagram Protocol. The packet bytes pane shows the raw data in hex and ASCII. The status bar at the bottom indicates the current packet and display statistics.

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

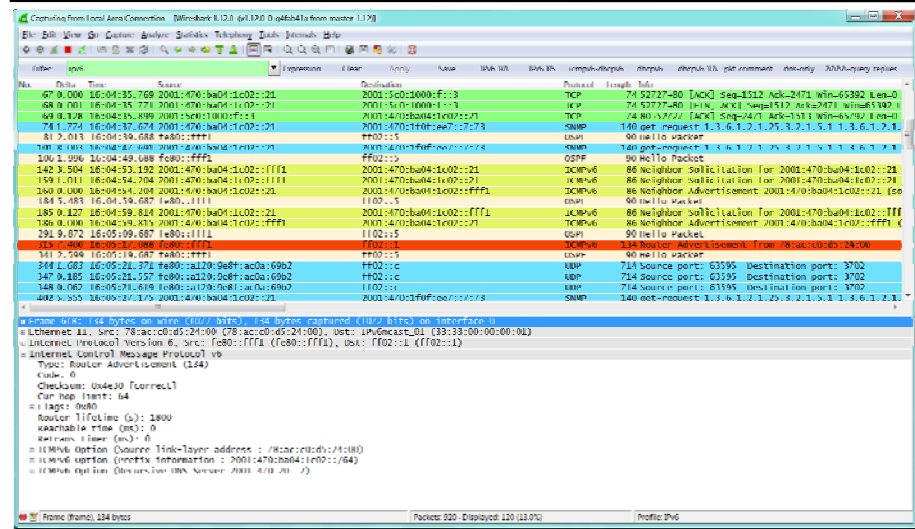
IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

68


IPv6 in Wireshark



Jeff's IPv6 Wireshark



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 69



Coloring rules

446	0.000	23:15:51.638	10.1.0.200	10.1.0.100	DNS	87	Standard query response	0x
447	0.000	23:15:51.638	10.1.0.200	10.1.0.100	DNS	87	Standard query response	0x
448	0.000	23:15:51.638	10.1.0.100	10.1.0.200	ICMP	115	Destination unreachable	0x
449	0.000	23:15:51.638	2001:db8:1ab:ba5e::2000	2001:db8:1ab:ba5e::102	DNS	96	Standard query response	0x
450	0.000	23:15:51.639	2001:db8:1ab:ba5e::102	2001:db8:1ab:ba5e::2000	ICMPv6	155	Destination unreachable	0x
451	0.959	23:15:52.599	Hewlett-b3:76:ec		LLDP_Multicast	282	Chassis Id = 00:16:35:b3:76:ec	0x
452	1.266	23:15:53.865	Fe80::1	ff02::1	ICMPv6	110	Router Advertisement from	0x
453	0.287	23:15:54.152	10.1.0.100	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1	0x
454	1.045	23:15:55.198	Hewlett-b3:76:c0	HP_00:00:67	HP	110	HP Switch Protocol	0x
455	1.130	23:15:56.328	Vmware_14:a9:fa	Vmware_10:59:5e	ARP	60	who has 10.1.0.200? Tell	0x
456	0.000	23:15:56.329	2001:db8:1ab:ba5e::102	2001:db8:1ab:ba5e::2000	ICMPv6	86	Neighbor Solicitation for	0x
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:	0x
458	0.000	23:15:56.331	2001:db8:1ab:ba5e::2000	2001:db8:1ab:ba5e::102	ICMPv6	86	Neighbor Advertisement 200	0x
459	0.810	23:15:57.141	10.1.0.100	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1	0x
460	2.999	23:16:00.141	10.1.0.100	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1	0x
461	3.012	23:16:03.153	10.1.0.100	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1	0x

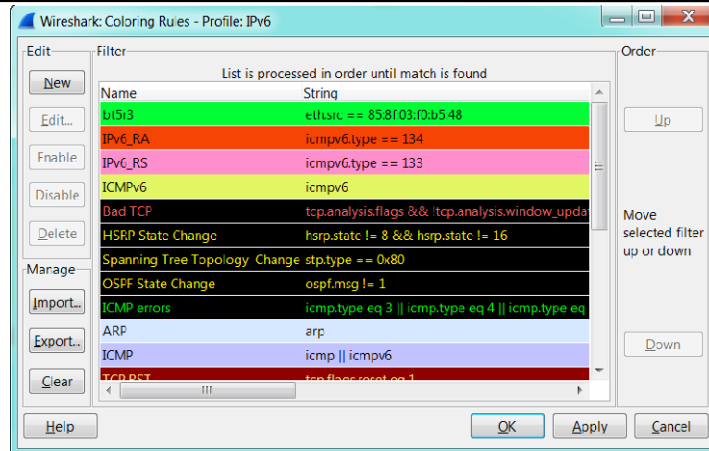
- Colors help you focus on specific address, protocols, events, and possibly find errors quickly

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 70

IPv6 in Wireshark



Color rule processing order

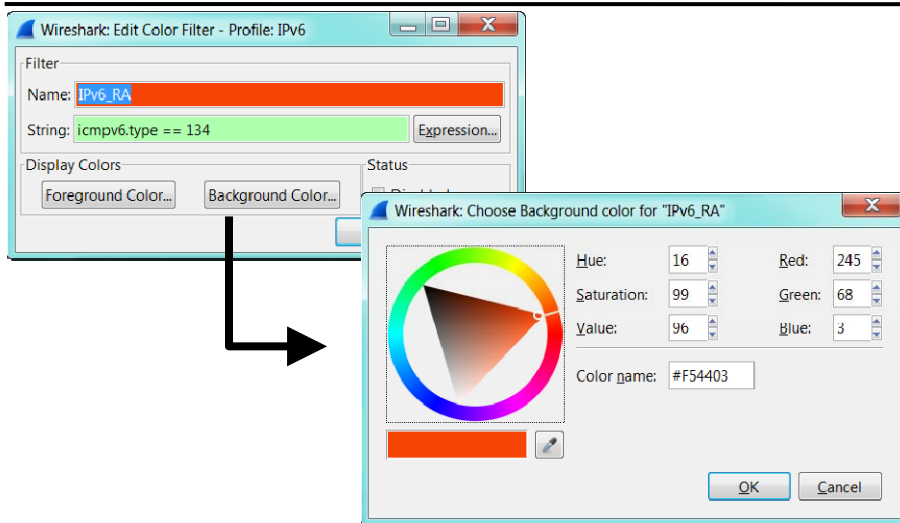


- Color rules read like a router ACL or firewall rule
 - First color rule that matches wins

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

71

Color rule creation



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

72

IPv6 in Wireshark

Columns

The first screenshot shows a packet list with columns: No., Delta, Time, and Source. A context menu is open over the 'Source' column heading, with 'Apply as Column' selected. The second screenshot shows the same packet list with a context menu open over the 'Time' column heading, showing options like 'Sort Ascending', 'Sort Descending', 'No Sorting', 'Align Left', 'Align Center', 'Align Right', 'Column Preferences...', 'Edit Column Details...', 'Resize Column', 'Displayed Columns', 'Hide Column', and 'Remove Column'.

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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 73

Display filters – option 1

The screenshot shows the Filter bar with a dropdown menu open. The filter 'icmp' is selected and highlighted in green. Below it, a list of filters is shown with their corresponding status colors: 'bootp' (red), 'ip.addr == 10.1.0.100 && dns' (green), 'pkt_comment' (yellow), 'dns' (red), 'ipv6' (green), 'dhcpv6 or icmpv6' (green), 'dhcpv6' (yellow), 'icmpv6.type == 134' (green), '((dns && udp.dstport != 5355)) && (dns.qry.name == "www' (green), and '...' (yellow).

- 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

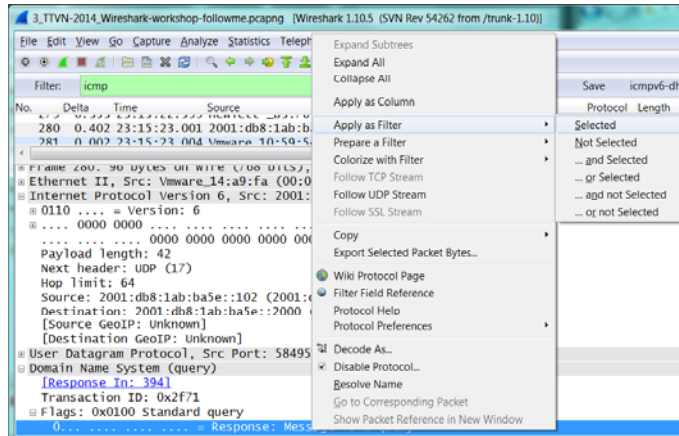
Filter: icmp Expression... Clear Apply Save icmpv6-dhcpv6 pkt_comment IPv6 dns_no-llmnr_www

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 74

IPv6 in Wireshark



Display filters – option 2



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

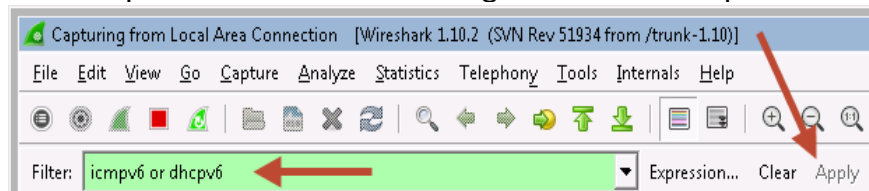
IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

75



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>



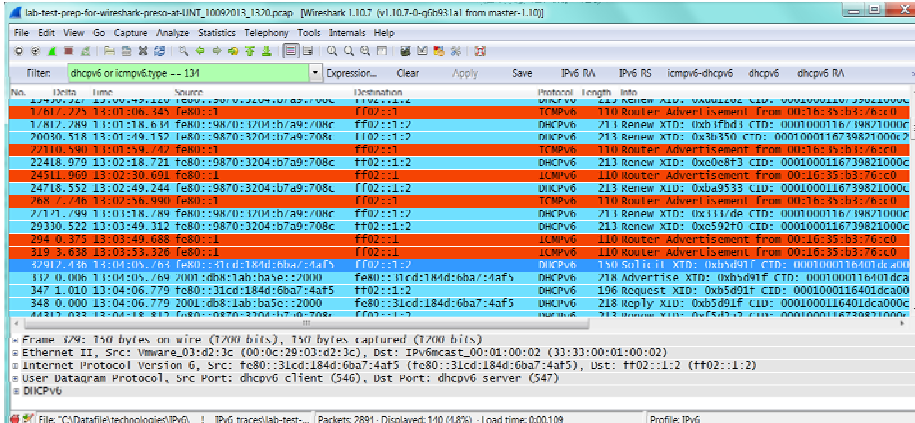
IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

76

IPv6 in Wireshark



Using Wireshark to view IPv6 pkts



lab-test-prep-for-wireshark-presso-at-INT_10097013_1520.pcap [Wireshark 1.10.7 (v1.10.7-0-g7b931a) from master-1.10]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `dhcpv6 or icmpv6type == 134` Expression... Clear Apply Save IPv6 RA IPv6 RS icmpv6-dhcpv6 dhcpv6 dhcpv6 RA

No.	Time	Source	Destination	Protocol	Length	Info
1761	2.25	13:02:06.445	fe80::1	ICMPv6	110	Router Advertisement From 00:10:35:03:76:c0
1762	2.89	13:02:18.634	fe80::9870:3204:b7a9:708c	DHCPv6	213	Renew XTID: 0xb1fbd1 CID: 0001000116739621000c
20050	518.13	01:09.152	fe80::9870:3204:b7a9:708c	DHCPv6	213	Renew XTID: 0xb350 CID: 0001000116739621000c
2210	591	11:01:29.742	fe80::1	ICMPv6	110	Router Advertisement From 00:10:35:03:76:c0
2248	970	13:02:18.721	fe80::9870:3204:b7a9:708c	DHCPv6	213	Renew XTID: 0xc08f3 CID: 0001000116739621000c
2451	969	13:02:30.691	fe80::1	ICMPv6	110	Router Advertisement From 00:10:35:03:76:c0
2478	552	13:02:49.244	fe80::9870:3204:b7a9:708c	DHCPv6	213	Renew XTID: 0xb9533 CID: 0001000116739621000c
265	496	18:02:25.890	fe80::1	ICMPv6	110	Router Advertisement From 00:10:35:03:76:c0
2717	194	11:01:28.789	fe80::9870:3204:b7a9:708c	DHCPv6	213	Renew XTID: 0x311d8 CID: 0001000116739621000c
2930	522	13:03:49.312	fe80::9870:3204:b7a9:708c	DHCPv6	213	Renew XTID: 0xc592f0 CID: 0001000116739621000c
294	0.375	13:03:49.688	fe80::1	ICMPv6	110	Router Advertisement From 00:10:35:03:76:c0
319	3.838	13:03:35.328	fe80::1	ICMPv6	110	Router Advertisement From 00:10:35:03:76:c0
3312	443	13:04:00.965	fe80::31cd:184d:6ba7:4af5	DHCPv6	106	Solicit XTID: 0xb5d01f CID: 0001000116401ca000
347	0.006	13:04:05.769	fe80::31cd:184d:6ba7:4af5	DHCPv6	218	Advertise XTID: 0xb5d01f CID: 0001000116401ca000
347	1.010	13:04:06.779	fe80::31cd:184d:6ba7:4af5	DHCPv6	106	Request XTID: 0xb5d01f CID: 0001000116401ca000
348	0.000	13:04:06.779	2001:db8:lab:ba3c::2000	DHCPv6	218	Reply XTID: 0xb5d01f CID: 0001000116401ca000c

Frame 374: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface vnet0/3

Ethernet II, Src: Vmware_03:d2:3c (00:0c:29:03:d2:3c), Dst: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)


Internet Protocol Version 6, Src: fe80::31cd:184d:6ba7:4af5 (fe80::31cd:184d:6ba7:4af5), Dst: ff02::1:2 (ff02::1:2)

User Datagram Protocol, Src Port: dhcpv6 client (547), Dst Port: dhcpv6 server (547)

DHCPv6

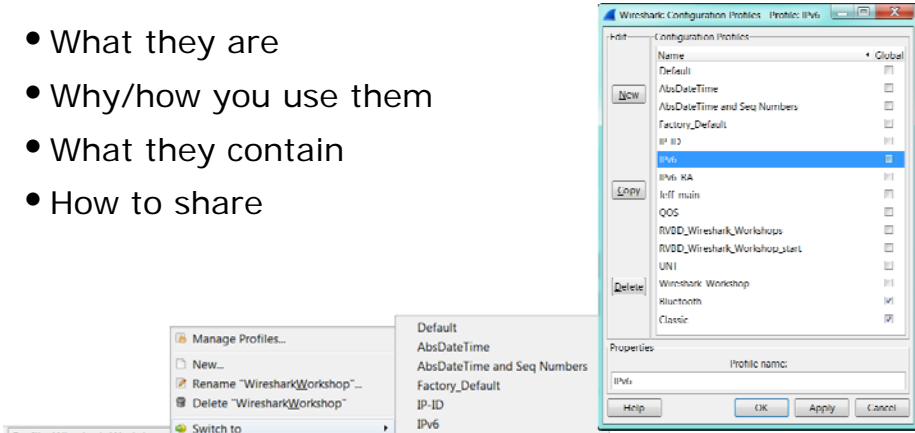
File: C:\Datafile\technology\IPv6__IPv6_trace\lab-test-... Packets: 2891 / Displayed: 140 (4.8%) / Load time: 0:00:109 Profile: IPv6

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 77



Configuration profiles

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



Wireshark: Configuration Profiles Profile: IPv6

Configuration Profiles

Name: Global

Default:

AbsDateTime:

AbsDateTime and Seq Numbers:

Factory_Default:

IP-ID:

IPv6:

IPv6 KA:

IPv6 main:

QOS:

RVDD_Wireshark_Workshops:

RVDD_Wireshark_Workshop_start:

UNT:

Wireshark_Workshop:

Bluetooth:

Classic:

Properties: Profile name: IPv6

Manage Profiles...

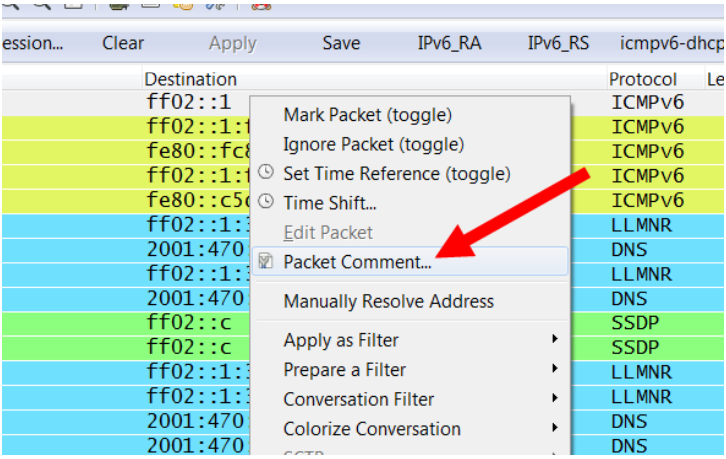
New...
Rename "WiresharkWorkshop" ...
Delete "WiresharkWorkshop" ...
Switch to: Wireshark_Workshop

Default
AbsDateTime
AbsDateTime and Seq Numbers
Factory_Default
IP-ID
IPv6
Jeff_main
UNT
• Wireshark_Workshop
New from Global

Profile: Wireshark_Workshop

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 78

IPv6 in Wireshark

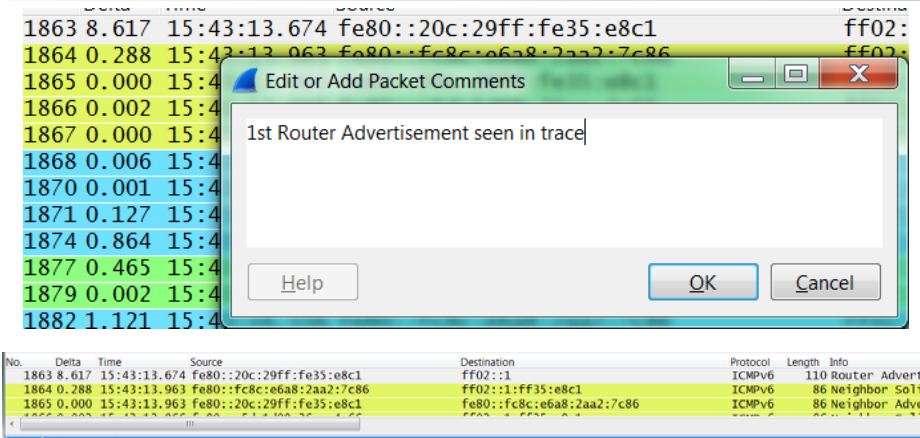


The screenshot shows the Wireshark packet list pane. A right-click context menu is open over a packet. The menu items include: Mark Packet (toggle), Ignore Packet (toggle), Set Time Reference (toggle), Time Shift..., Edit Packet, Packet Comment..., Manually Resolve Address, Apply as Filter, Prepare a Filter, Conversation Filter, and Colorize Conversation. A red arrow points to the 'Packet Comment...' option. The background shows a list of packets with columns for No., Time, Source, Destination, Protocol, and Length.

Packet annotation

- Right click packet, select Packet Comment

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 79



The screenshot shows the same Wireshark packet list pane. An 'Edit or Add Packet Comments' dialog box is open, displaying the text '1st Router Advertisement seen in trace'. The dialog has 'Help', 'OK', and 'Cancel' buttons. The background shows the packet list with columns for No., Delta, Time, Source, Destination, Protocol, Length, and Info.

Packet annotation

1st Router Advertisement seen in trace

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 80

IPv6 in Wireshark



Wireshark demo #1 – watch me

- Discussion about various IPv6 operations and viewing them in Wireshark



Wireshark demo #2 – follow me

- Open:
 - “Troopers2015_Wireshark-workshop.pcapng”
- Watch and follow me on this one
 - Telnet
 - SSH
 - HTTP
 - DNS
- Now it's your turn...next slide please

IPv6 in Wireshark



Wireshark lab #1

- Create your own named profile
- Add delta time column
- Change time/date to time (only) and in milliseconds
- Create/save pkt_comment filter

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

83



Wireshark lab #2

- Find 1st pkt with dns.qry.name == "www.ipv6sandbox.com"
 - make a note as to which pkt this is
- Find 1st pkt with AAAA 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 v1.2 - Copyright © 2015 Jeffrey L. Carrell

84

IPv6 in Wireshark



Wireshark lab #3

- 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
- Find pkt with comment of 'this is the secret pkt with the most important comment!'

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

85



Wireshark lab #4 – IPv6-RA

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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

86

IPv6 in Wireshark



Wireshark lab #5 – DHCPv6

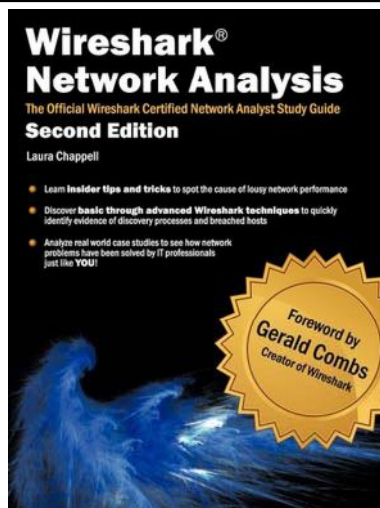
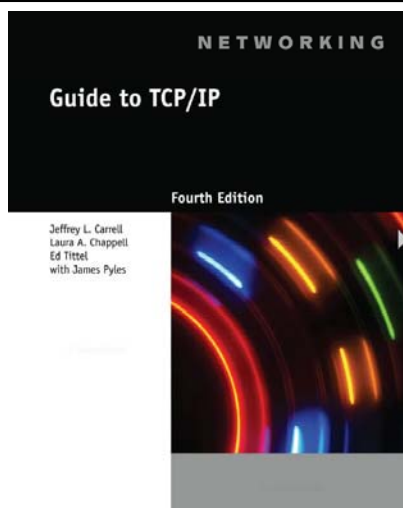
- Inspect DHCPv6 packets
 - configure a display filter as “dhcpv6”
 - pick a specific client
 - find the first of each of its DHCPv6 process pkts
 - what is the dhcpv6 server’s v6 addr?
 - what are the pkt numbers for:
Solicit ____ Advertise ____ Request ____ Reply ____
 - what v6 addr did the client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

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

87



Resources



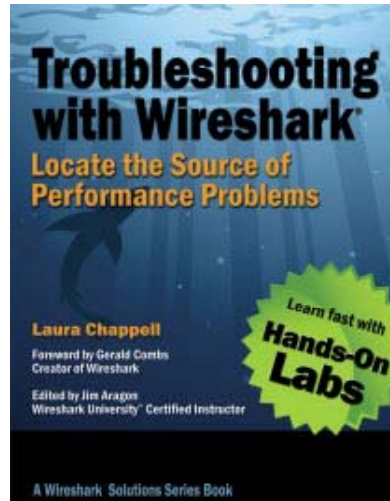
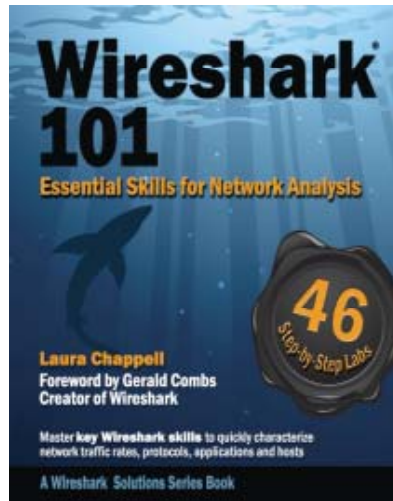
IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

88

IPv6 in Wireshark



Resources

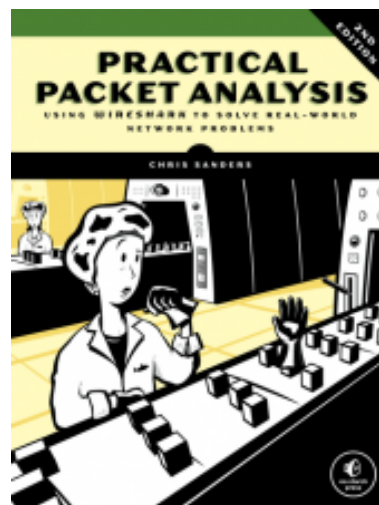
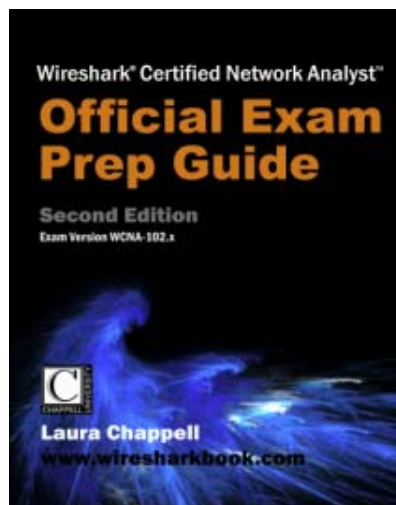


IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell

89






Resources



IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell


90

IPv6 in Wireshark

Resources

O'REILLY



IPv6 Address Planning

DESIGNING AN ADDRESS PLAN FOR THE FUTURE

Tom Coffeen

THE EXPERT'S VOICE® IN NETWORKING

Practical IPv6 for Windows Administrators

GET UP TO SPEED ON THE FUTURE OF THE INTERNET WITH A FAST, PRACTICAL REFERENCE TO IPv6

Edward Horley
Foreword by Stephen L. Rose

Apress®

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 91

Resources

 CISCO

IPv6 Fundamentals

A Straightforward Approach to Understanding IPv6



rickgraziani.com

Rick Graziani

Microsoft

Understanding IPv6




3rd Edition



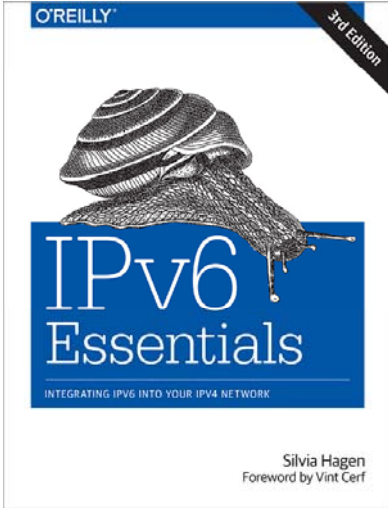
Joseph Davies

IPv6 in Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 92

IPv6 in Wireshark

Resources



IPV6 In Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 93

Thank You for Attending!

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




IPV6 In Wireshark v1.2 - Copyright © 2015 Jeffrey L. Carrell 94