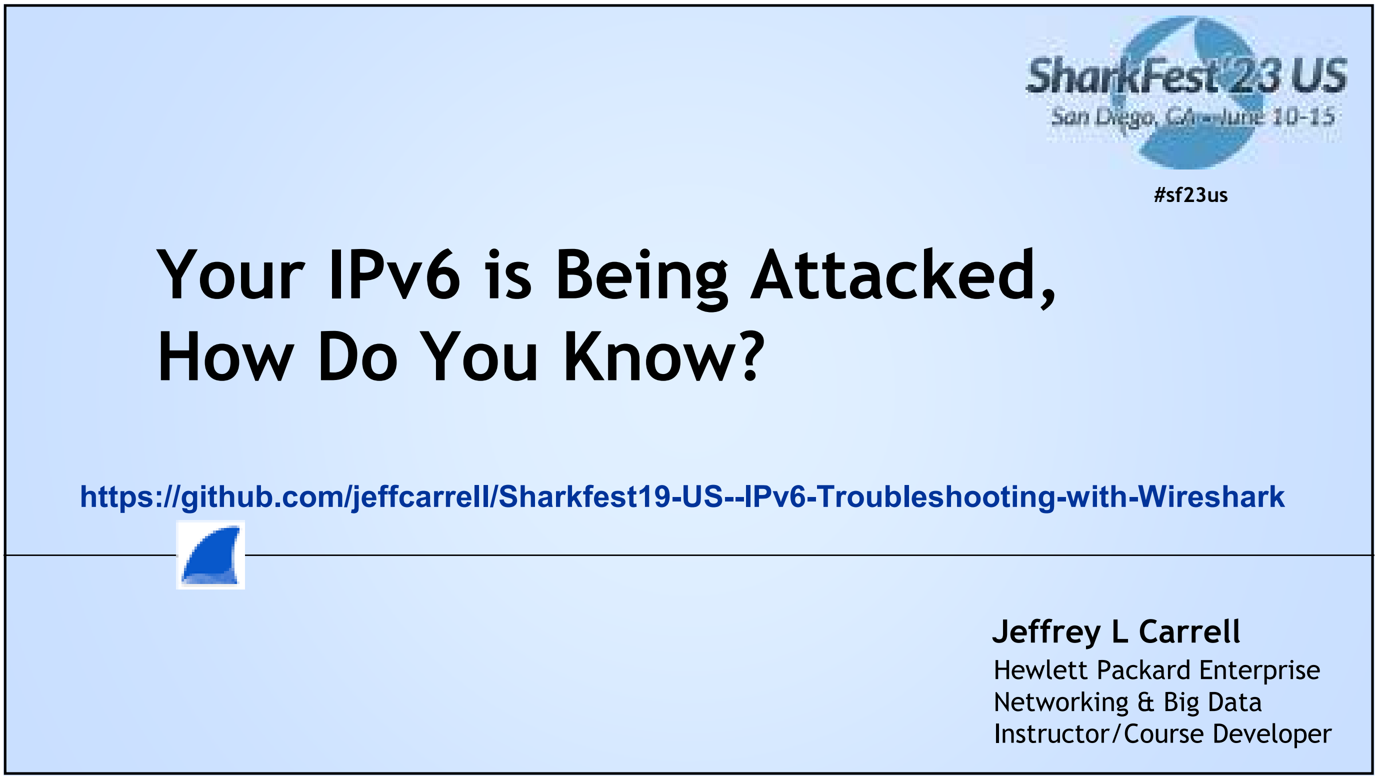


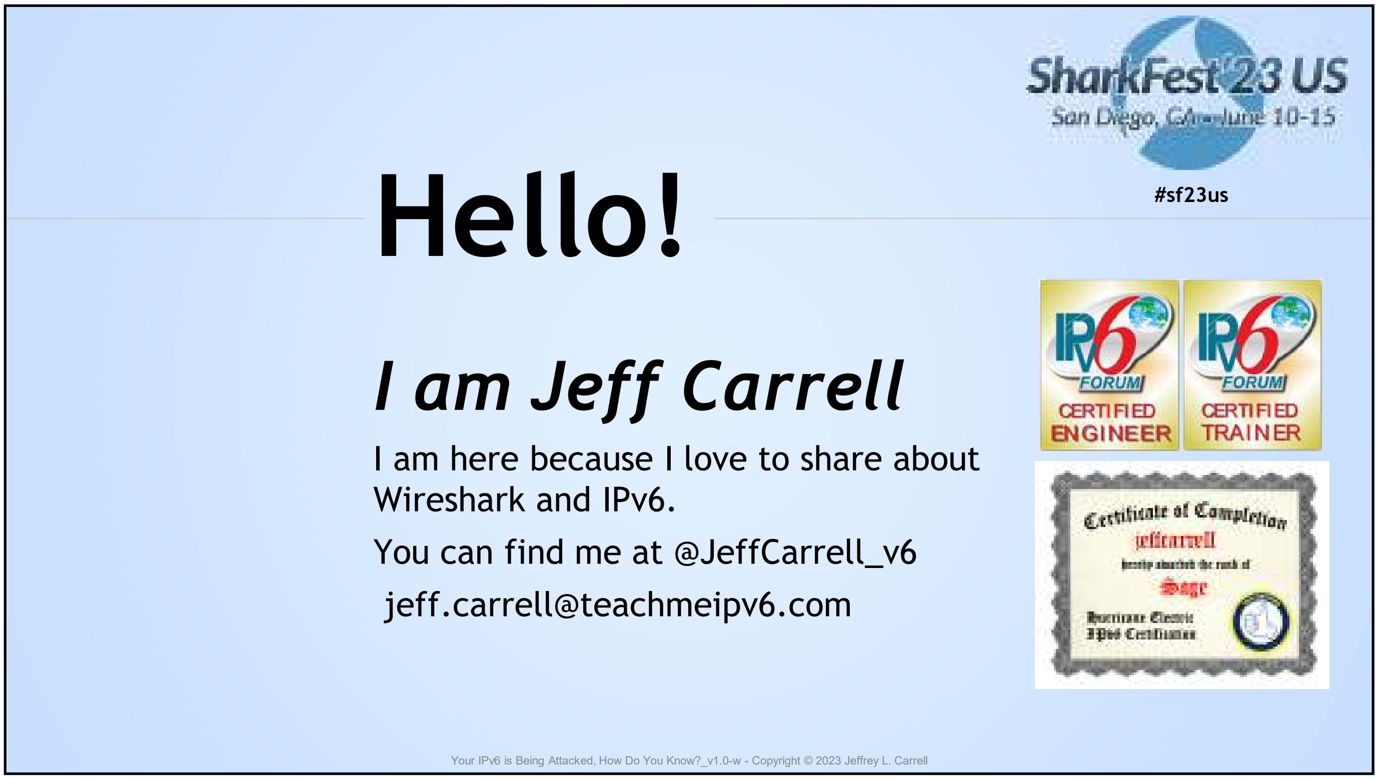
SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

Your IPv6 is Being Attacked, How Do You Know?

https://github.com/jeffcarrell/Sharkfest19-US--IPv6-Troubleshooting-with-Wireshark

Jeffrey L Carrell
Hewlett Packard Enterprise
Networking & Big Data
Instructor/Course Developer



SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

Hello!

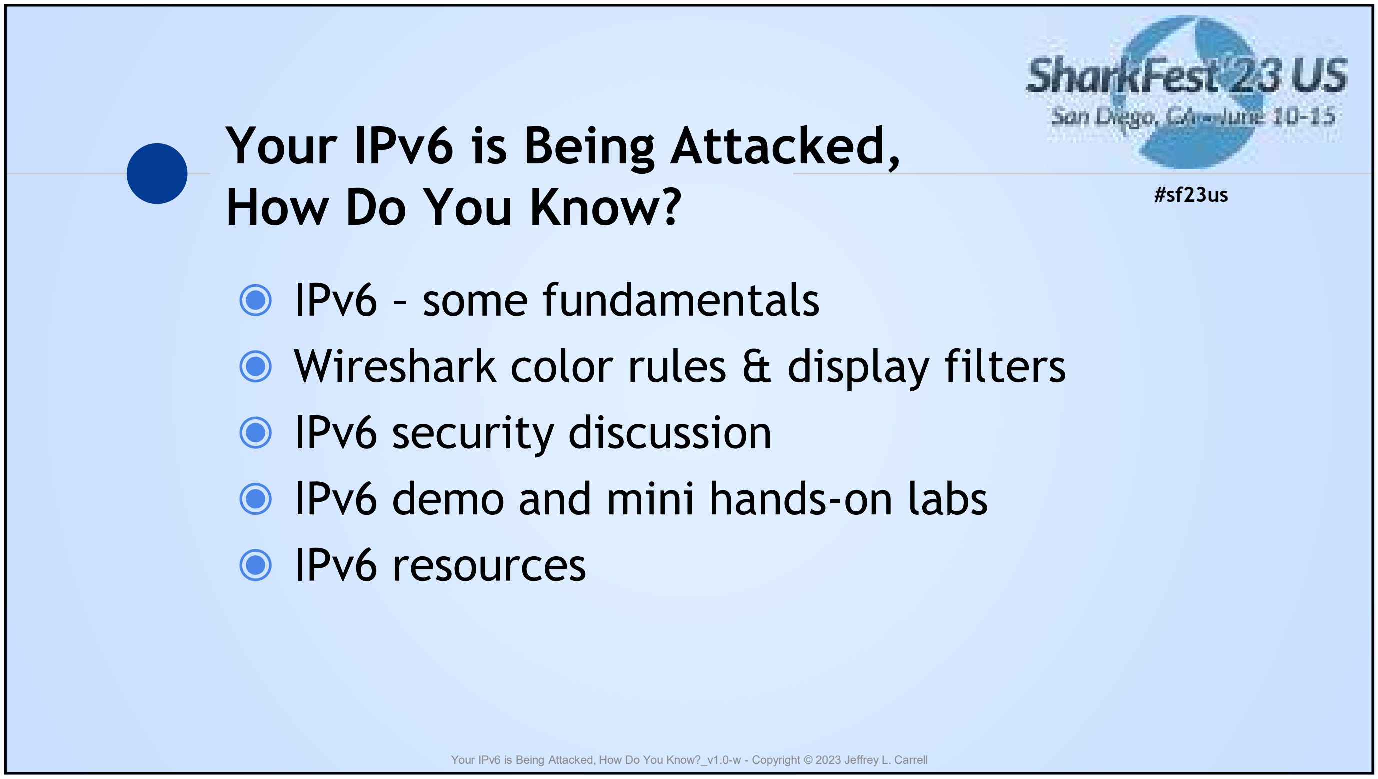
I am Jeff Carrell

I am here because I love to share about Wireshark and IPv6.

You can find me at @JeffCarrell_v6

jeff.carrell@teachmeipv6.com

IPv6 FORUM CERTIFIED ENGINEER
IPv6 FORUM CERTIFIED TRAINER
Certificate of Completion
jeffcarrell
hereby awarded the rank of
Sage
Hurricane Electric
IPv6 Certification

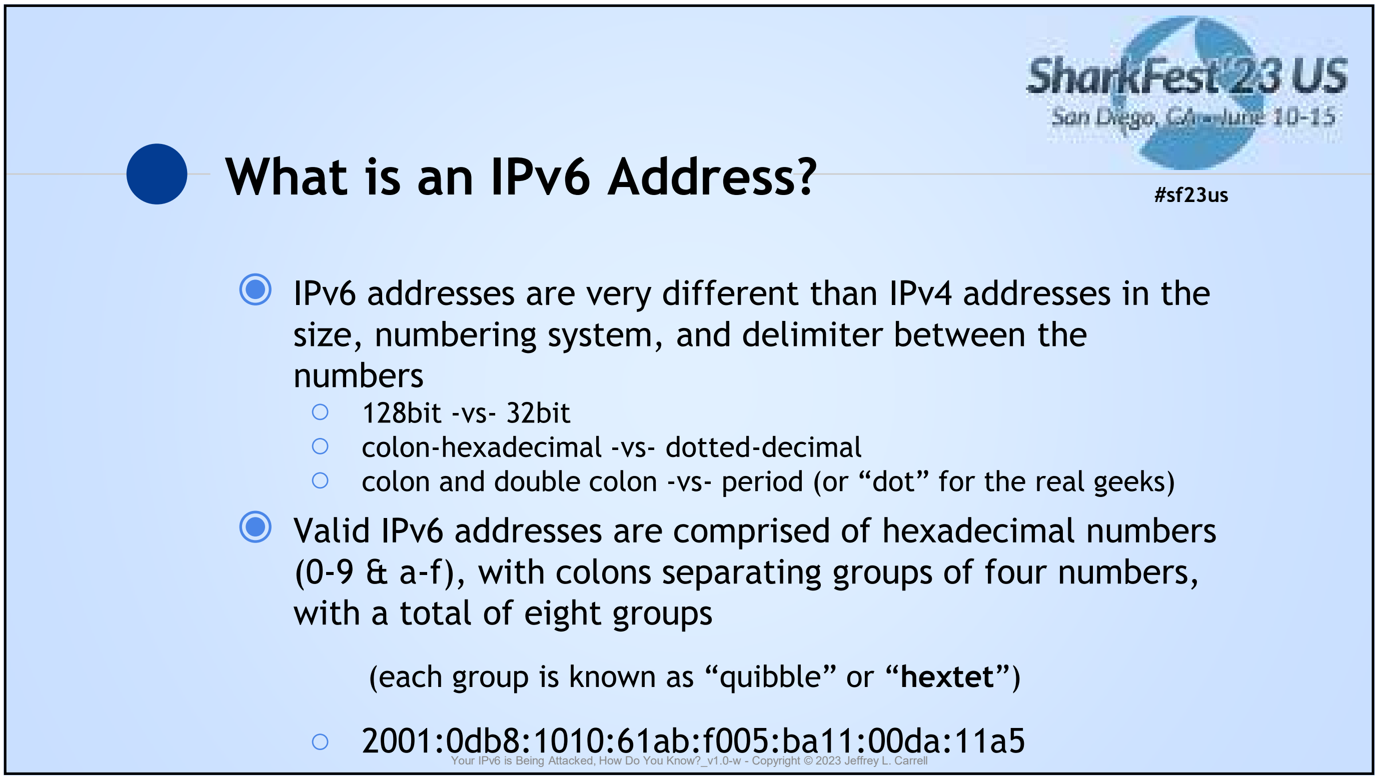


SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Your IPv6 is Being Attacked, How Do You Know?

- IPv6 – some fundamentals
- Wireshark color rules & display filters
- IPv6 security discussion
- IPv6 demo and mini hands-on labs
- IPv6 resources



SharkFest'23 US
San Diego, CA • June 10-15

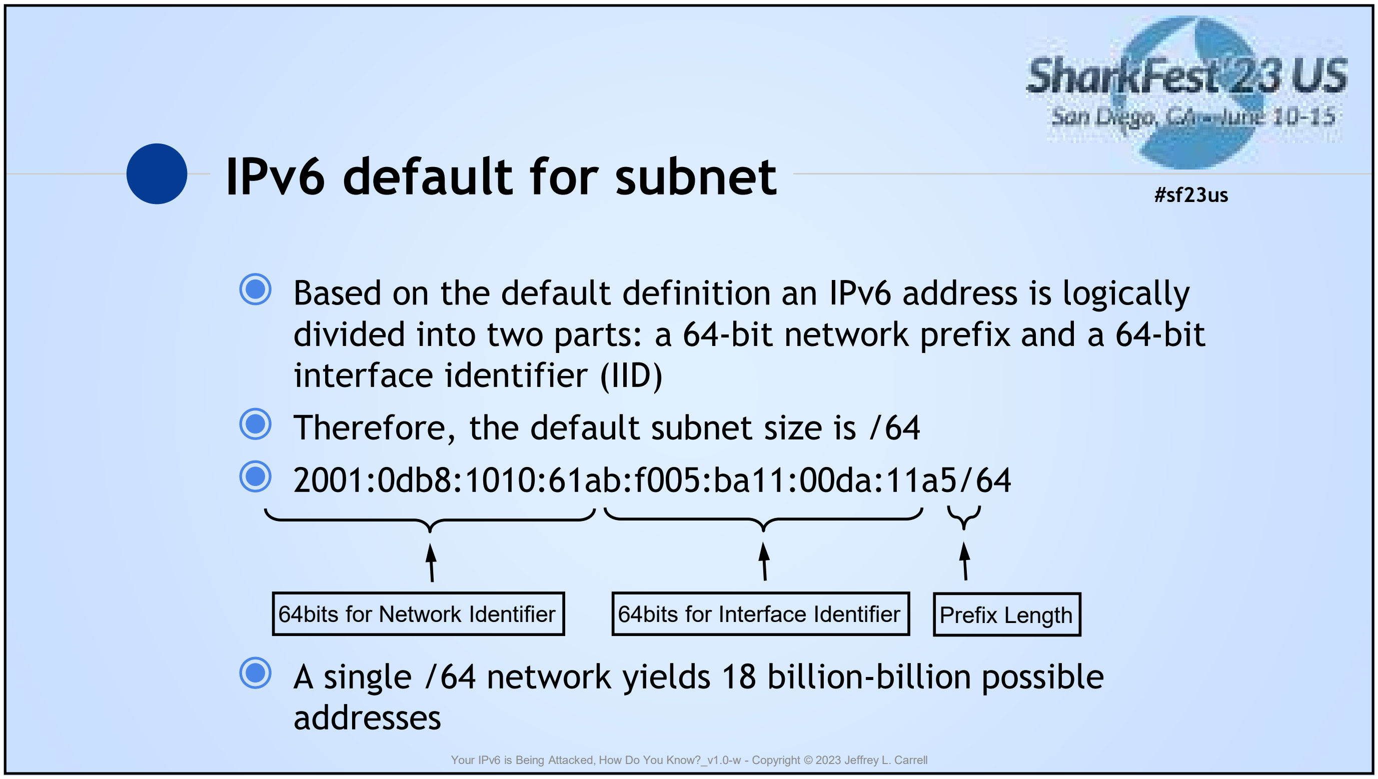
#sf23us

What is an IPv6 Address?

- IPv6 addresses are very different than IPv4 addresses in the size, numbering system, and delimiter between the numbers
  - 128bit -vs- 32bit
  - colon-hexadecimal -vs- dotted-decimal
  - colon and double colon -vs- period (or "dot" for the real geeks)
- Valid IPv6 addresses are comprised of hexadecimal numbers (0-9 & a-f), with colons separating groups of four numbers, with a total of eight groups

  (each group is known as "quibble" or "**hextet**")

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



IPv6 default for subnet

#sf23us

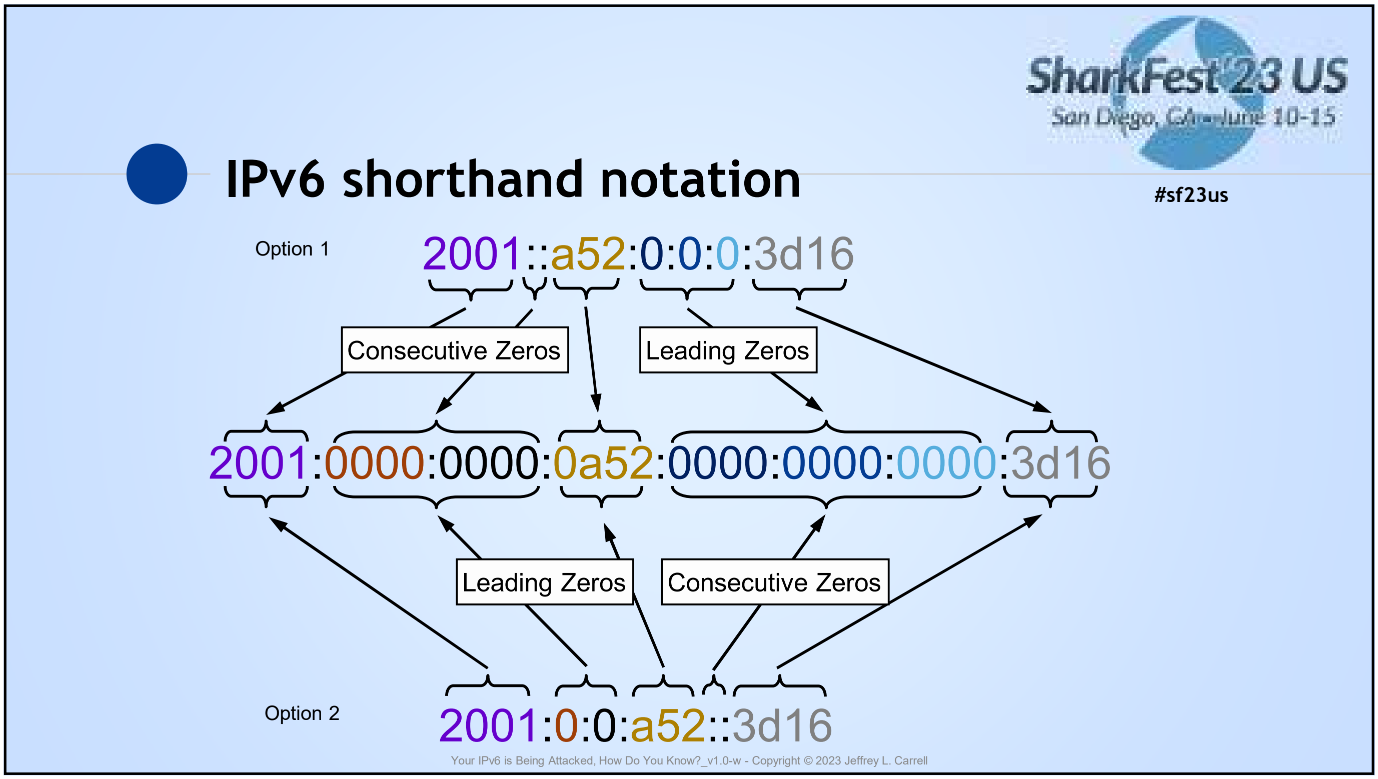
- Based on the default definition an IPv6 address is logically divided into two parts: a 64-bit network prefix and a 64-bit interface identifier (IID)
- Therefore, the default subnet size is /64
- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64

64bits for Network Identifier

64bits for Interface Identifier

Prefix Length

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



IPv6 shorthand notation

#sf23us

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

Consecutive Zeros

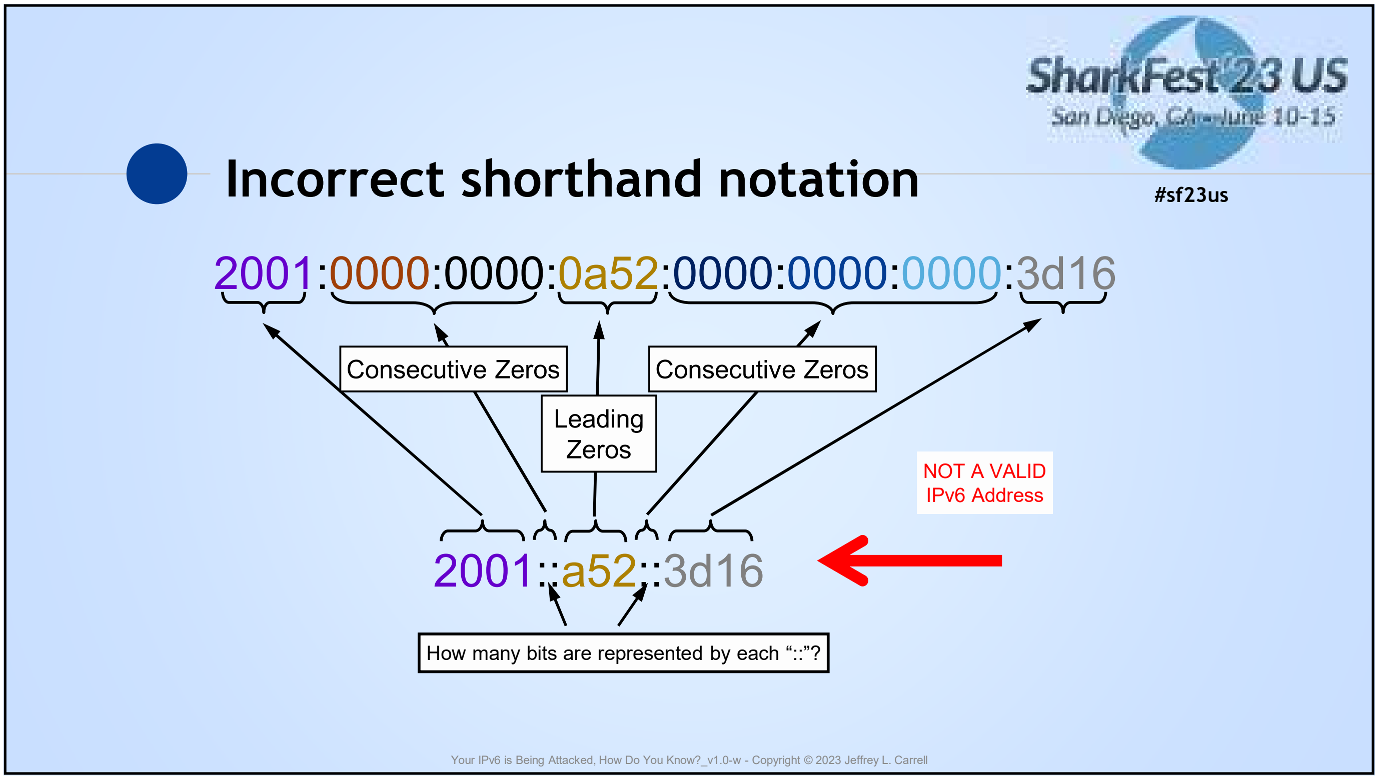
Leading Zeros

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

Leading Zeros

Consecutive Zeros

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



Incorrect shorthand notation

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

Consecutive Zeros

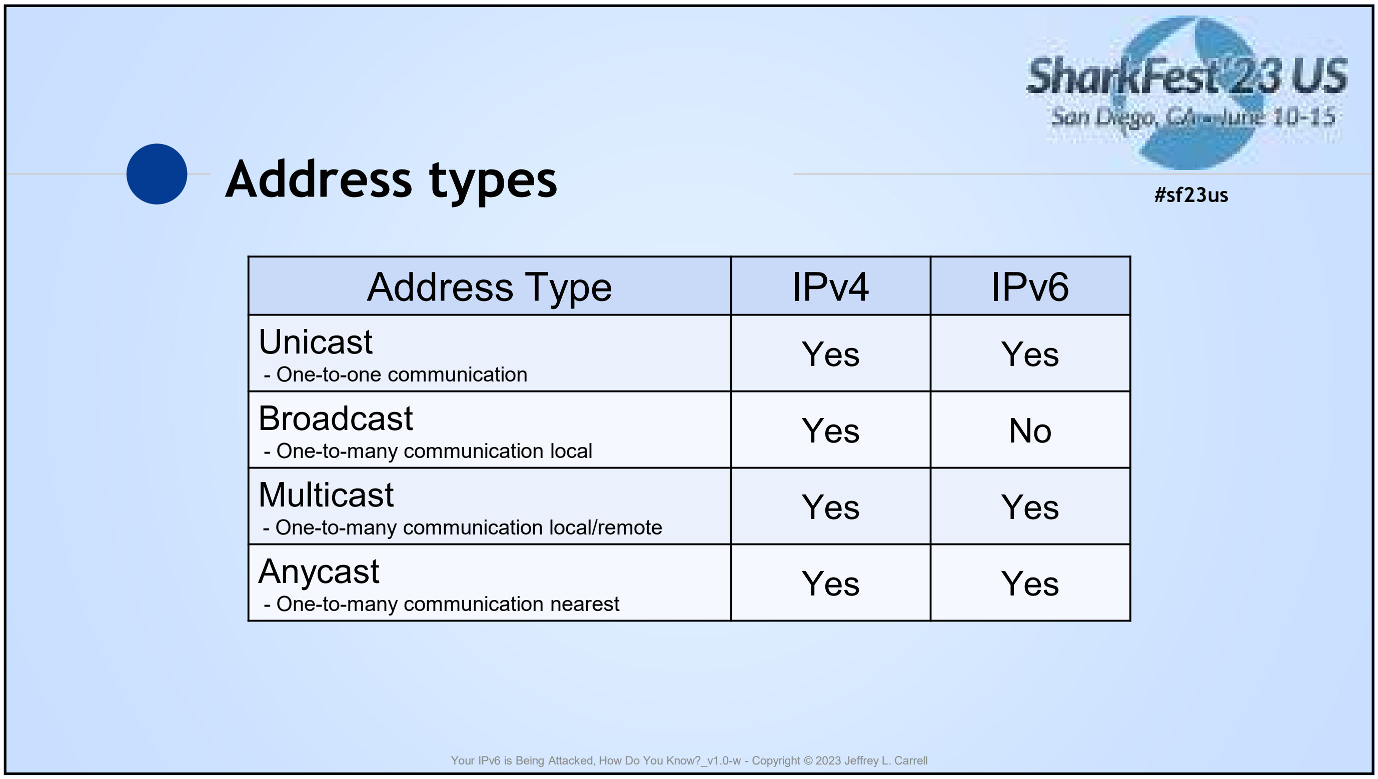
Leading Zeros

Consecutive Zeros

2001::a52::3d16

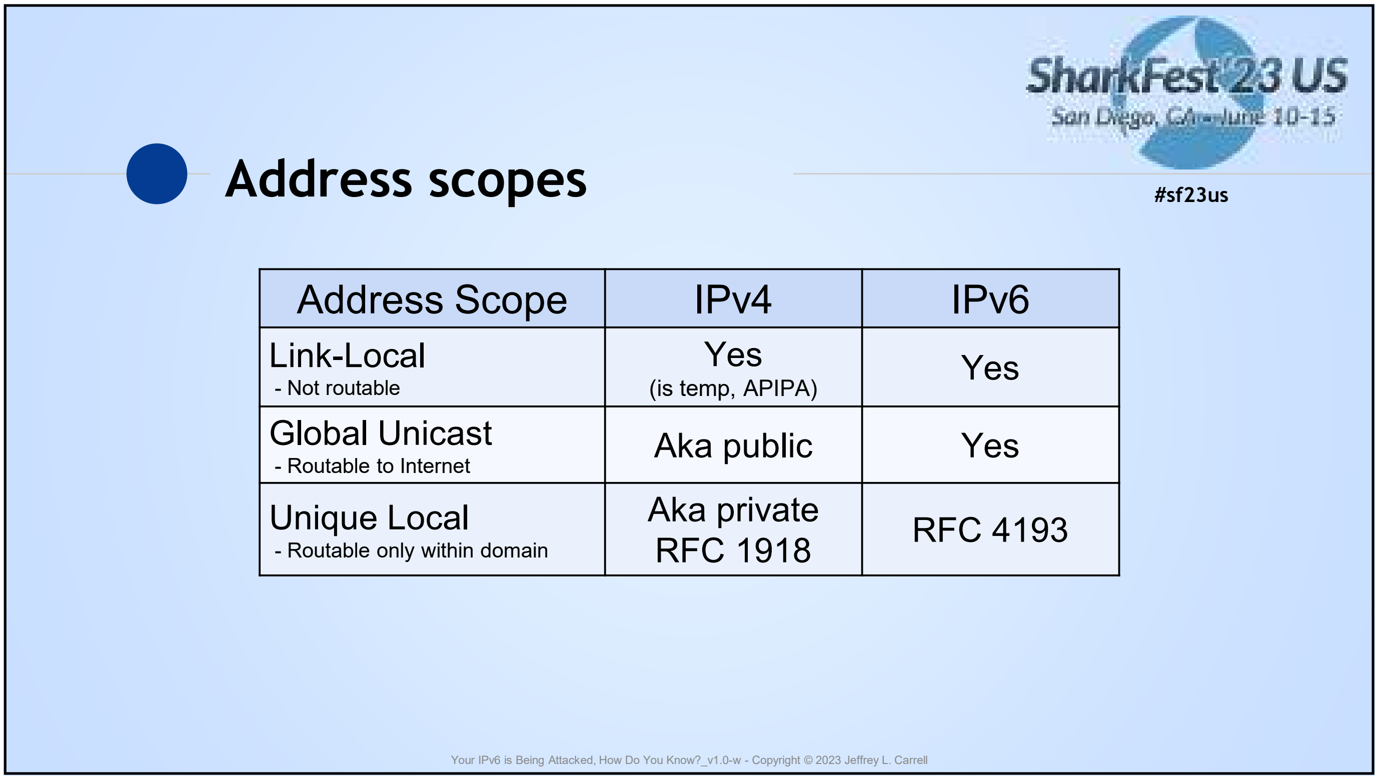
NOT A VALID IPv6 Address

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


SharkFest'23 US
San Diego, CA • June 10-15
#sf23us

Address types

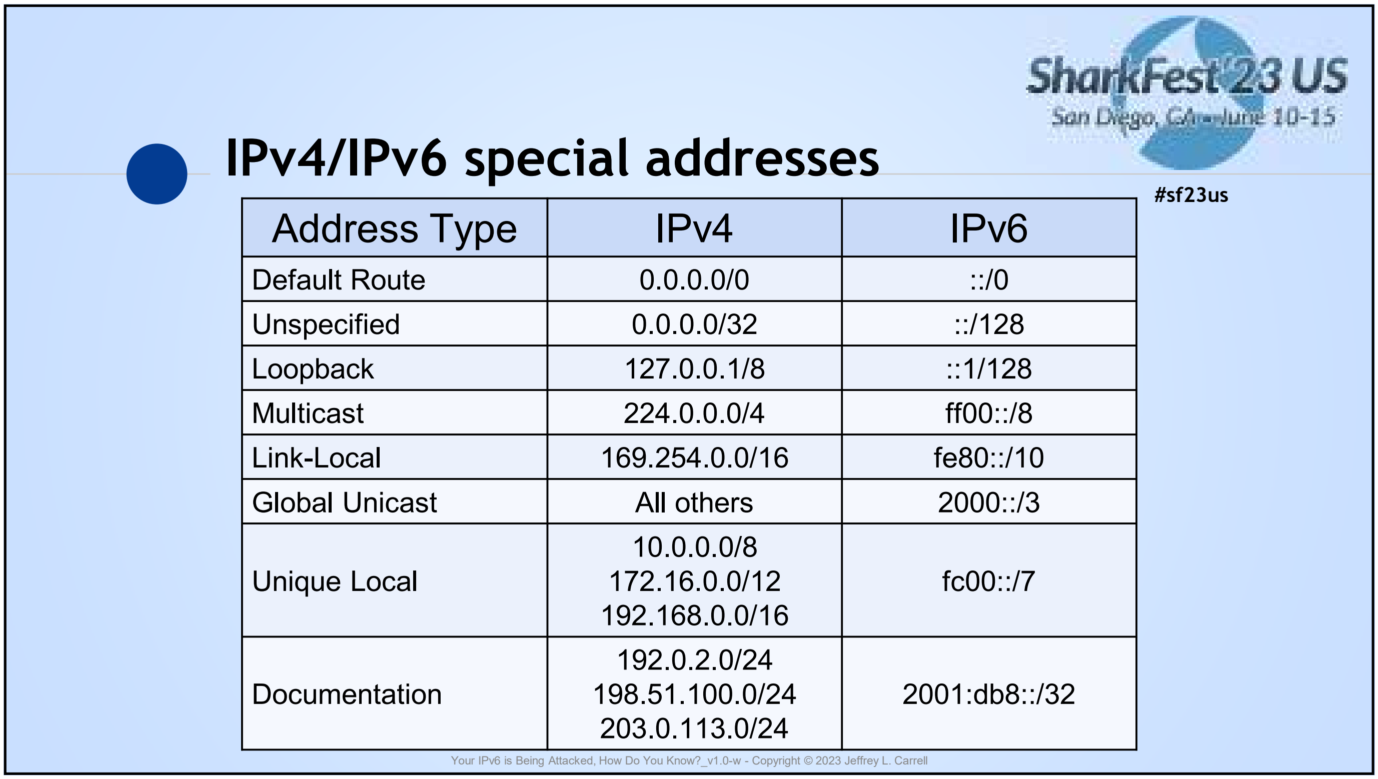
Address Type	IPv4	IPv6
Unicast - One-to-one communication	Yes	Yes
Broadcast - One-to-many communication local	Yes	No
Multicast - One-to-many communication local/remote	Yes	Yes
Anycast - One-to-many communication nearest	Yes	Yes



#sf23us

Address scopes

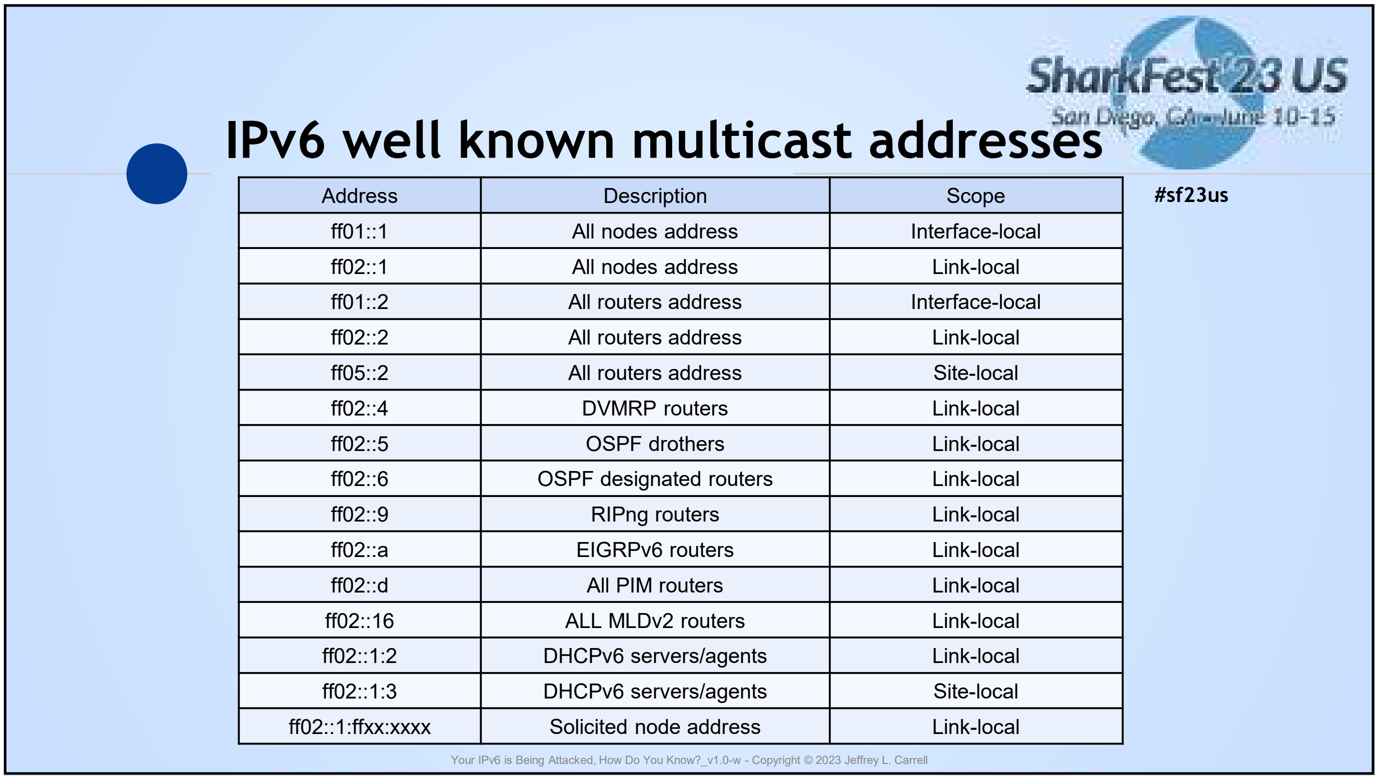
Address Scope	IPv4	IPv6
Link-Local - Not routable	Yes (is temp, APIPA)	Yes
Global Unicast - Routable to Internet	Aka public	Yes
Unique Local - Routable only within domain	Aka private RFC 1918	RFC 4193



#sf23us

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

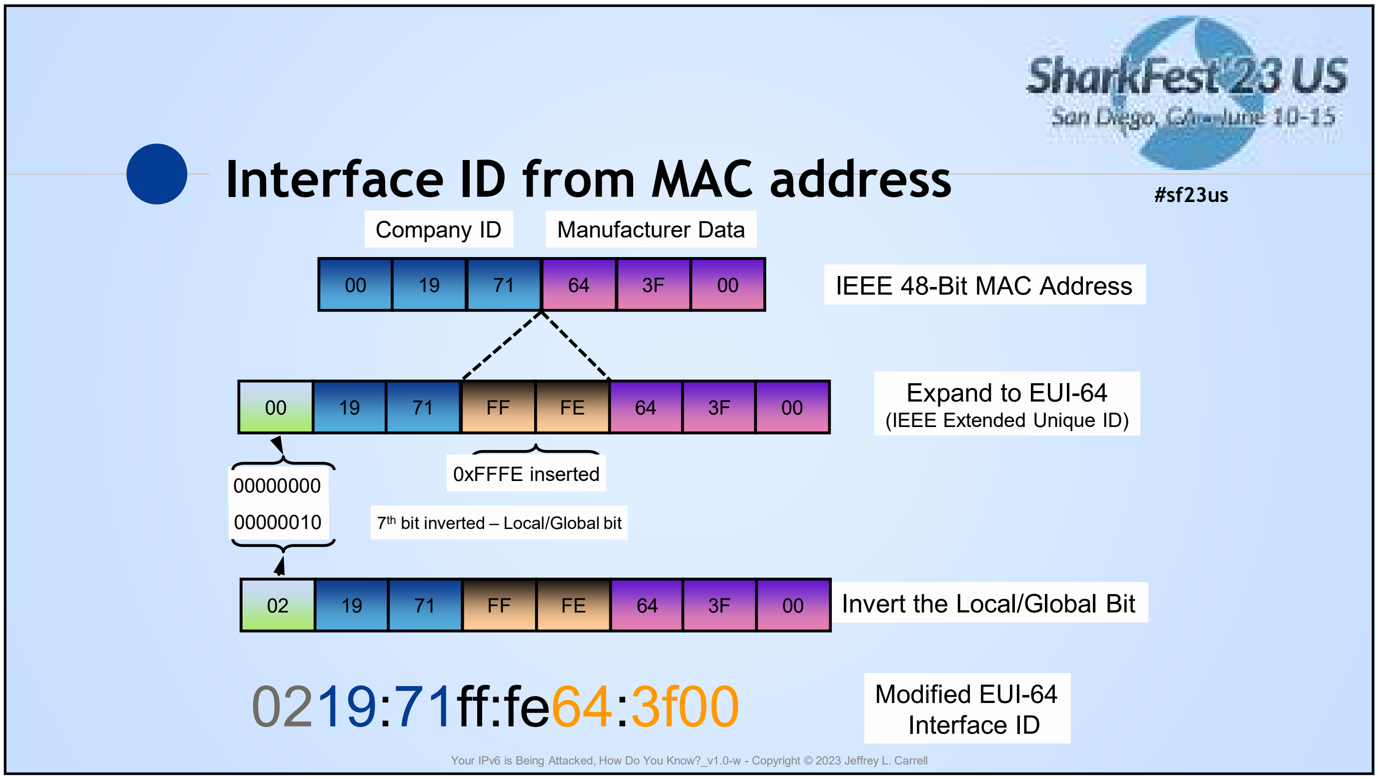


SharkFest'23 US
San Diego, CA – June 10-15

IPv6 well known multicast addresses

#sf23us

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



SharkFest'23 US
San Diego, CA – June 10-15

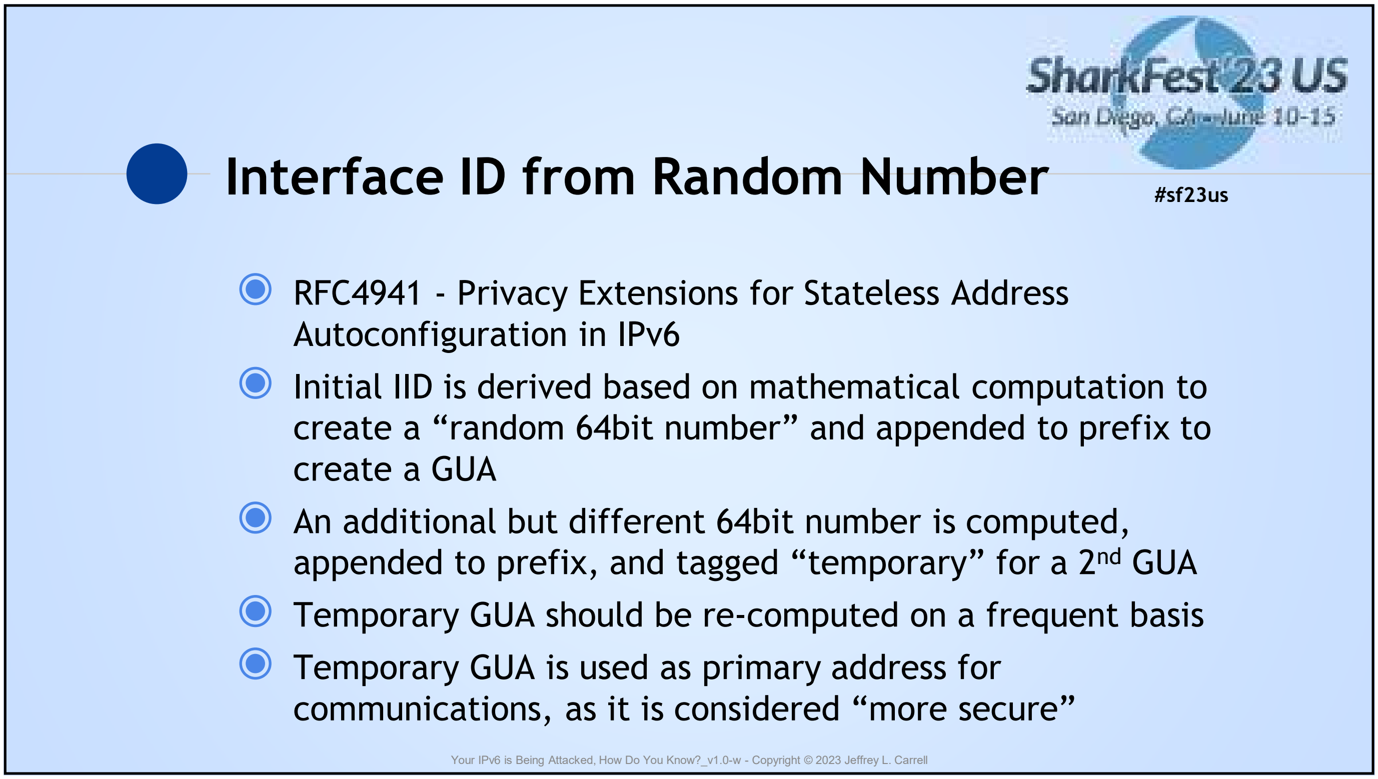
Interface ID from MAC address

#sf23us

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

0219:71ff:fe64:3f00

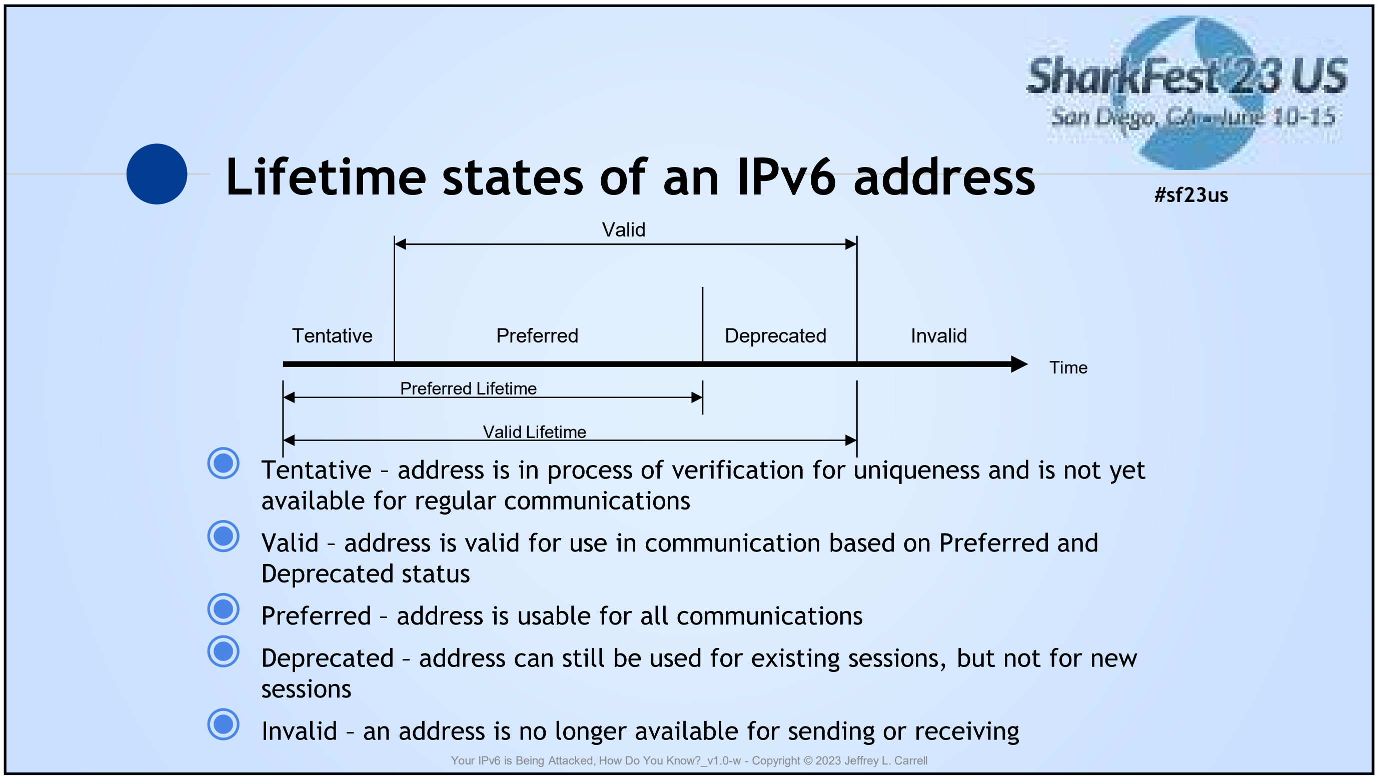
Modified EUI-64
Interface ID



Interface ID from Random Number

#sf23us

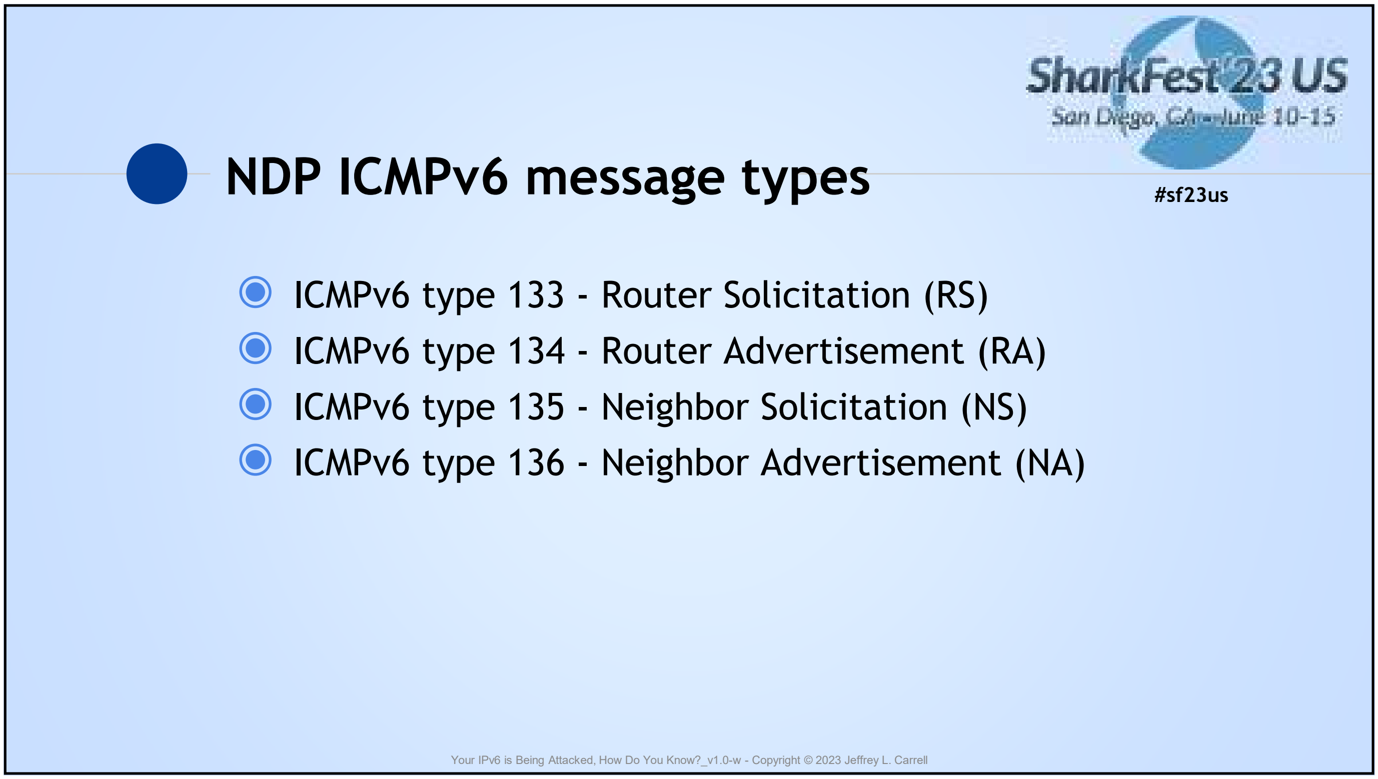
- RFC4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- Initial IID is derived based on mathematical computation to create a “random 64bit number” and appended to prefix to create a GUA
- An additional but different 64bit number is computed, appended to prefix, and tagged “temporary”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

#sf23us

- 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

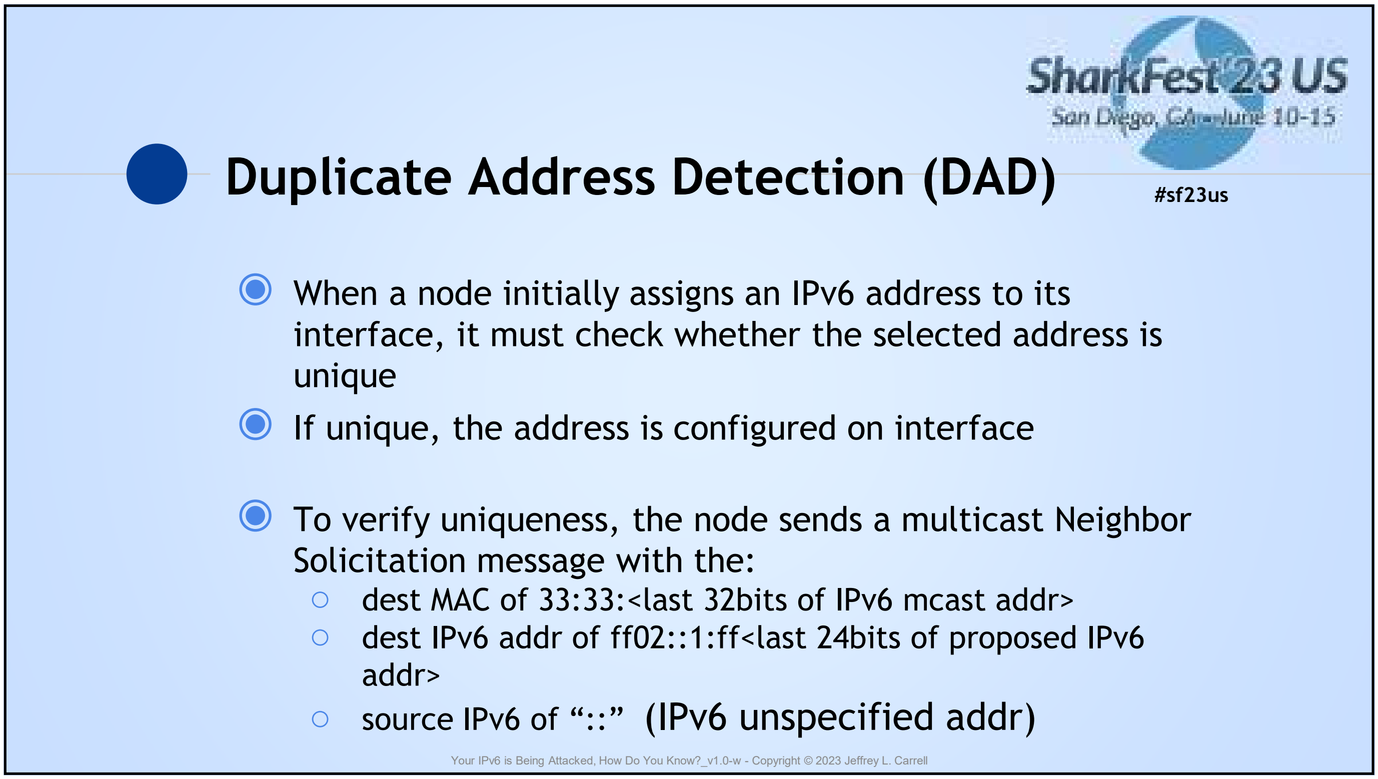


SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

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)

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell



SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

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)

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

SharkFest'23 US
San Diego, CA – June 10-15

IPv6 autoconfiguration options

#sf23us

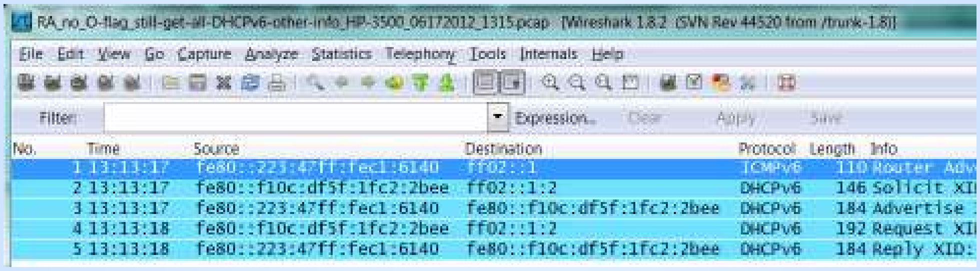
Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options	# of IPv6 Addr
	M Flag	O Flag	A Flag	L Flag				
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::)	M-EUI-64 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)

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

SharkFest'23 US
San Diego, CA – June 10-15

IPv6 Stateful (DHCPv6) process

#sf23us


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

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

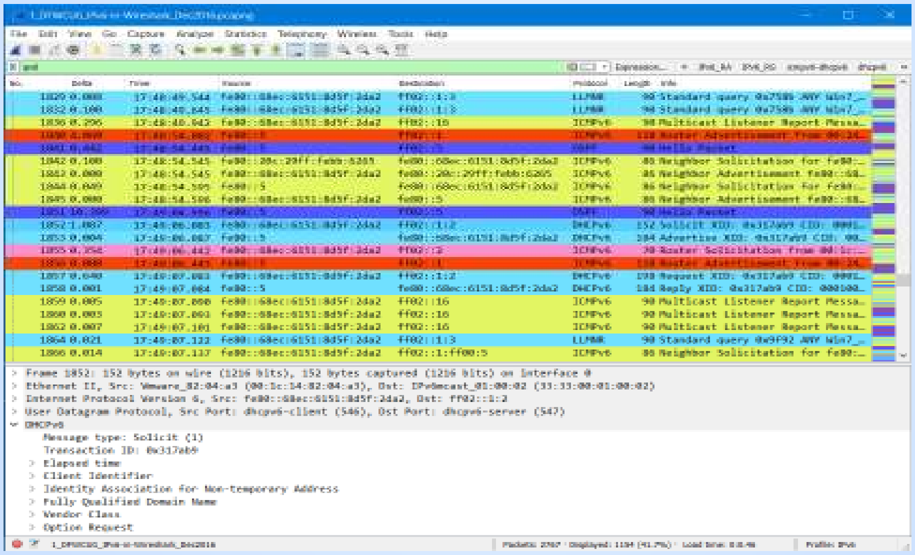
- DHCPv6Solicit = DHCPDiscover (IPv4)
- DHCPv6Advertise = DHCPOffer (IPv4)
- DHCPv6Request = DHCPRequest (IPv4)
- DHCPv6Reply = DHCPAck (IPv4)

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

SharkFest'23 US
San Diego, CA – June 10-15

Jeff's IPv6 Wireshark

#sf23us



```
No.   Delta   Time          Source                        Destination                   Protocol Length Info
 1829 0.000   17:48:49.544  fe80::68ec:6151:8d5f:2da2     ff02::1:3                     LLMNR    90 Standard query 0a7586 ANY Win7_…
 1832 0.100   17:48:49.645  fe80::68ec:6151:8d5f:2da2     ff02::1:3                     LLMNR    90 Standard query 0a7586 ANY Win7_…
 1836 0.296   17:48:49.942  fe80::68ec:6151:8d5f:2da2     ff02::16                      ICMPv6   90 Multicast Listener Report Messa…
 1838 8.869   17:48:54.002  fe80::5                       ff02::1                       ICMPv6  118 Router Advertisement from 00:24…
 1841 0.443   17:48:54.443  fe80::5                       ff02::5                       OSPF     90 Hello Packet
 1842 0.100   17:48:54.545  fe80::20c:29ff:febb:6265      fe80::68ec:6151:8d5f:2da2     ICMPv6   86 Neighbor Solicitation for fe80:…
 1842 0.000   17:48:54.545  fe80::68ec:6151:8d5f:2da2     fe80::20c:29ff:febb:6265      ICMPv6   86 Neighbor Advertisement fe80::68…
 1844 0.049   17:48:54.595  fe80::5                       fe80::68ec:6151:8d5f:2da2     ICMPv6   86 Neighbor Solicitation for fe80:…
 1845 0.000   17:48:54.596  fe80::68ec:6151:8d5f:2da2     fe80::5                       ICMPv6   86 Neighbor Advertisement fe80::68…
 1851 10.390  17:49:06.496  fe80::5                       ff02::5                       OSPF     90 Hello Packet
 1852 1.087   17:49:06.083  fe80::68ec:6151:8d5f:2da2     ff02::1:2                     DHCPv6  152 Solicit XID: 0x317ab9 CID: 0001…
 1853 0.004   17:49:06.087  fe80::5                       fe80::68ec:6151:8d5f:2da2     DHCPv6  184 Advertise XID: 0x317ab9 CID: 00…
 1855 0.356   17:49:06.443  fe80::68ec:6151:8d5f:2da2     ff02::2                       ICMPv6   70 Router Solicitation from 00:1c:…
 1856 0.000   17:49:06.443  fe80::5                       ff02::1                       ICMPv6  118 Router Advertisement from 00:24…
 1857 0.640   17:49:07.083  fe80::68ec:6151:8d5f:2da2     ff02::1:2                     DHCPv6  198 Request XID: 0x317ab9 CID: 0001…
 1858 0.001   17:49:07.084  fe80::5                       fe80::68ec:6151:8d5f:2da2     DHCPv6  184 Reply XID: 0x317ab9 CID: 000100…
 1859 0.005   17:49:07.088  fe80::68ec:6151:8d5f:2da2     ff02::16                      ICMPv6   90 Multicast Listener Report Messa…
 1860 0.003   17:49:07.091  fe80::68ec:6151:8d5f:2da2     ff02::16                      ICMPv6   90 Multicast Listener Report Messa…
 1862 0.007   17:49:07.101  fe80::68ec:6151:8d5f:2da2     ff02::16                      ICMPv6   90 Multicast Listener Report Messa…
 1864 0.021   17:49:07.122  fe80::68ec:6151:8d5f:2da2     ff02::1:3                     LLMNR    90 Standard query 0x9f92 ANY Win7_…
 1866 0.014   17:49:07.137  fe80::68ec:6151:8d5f:2da2     ff02::1:ff00:5                ICMPv6   86 Neighbor Solicitation for fe80:…
```

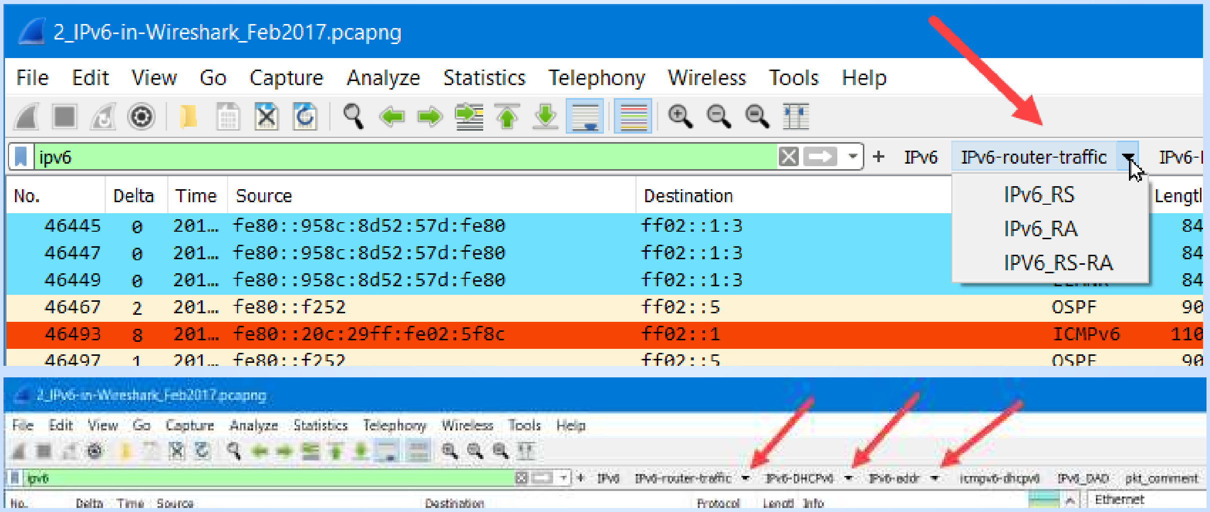
```
> Frame 1852: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
> Ethernet II, Src: Vmware_82:04:a3 (00:1c:14:82:04:a3), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::68ec:6151:8d5f:2da2, Dst: ff02::1:2
> User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
v DHCPv6
    Message type: Solicit (1)
    Transaction ID: 0x317ab9
  > Elapsed time
  > Client Identifier
  > Identity Association for Non-temporary Address
  > Fully Qualified Domain Name
  > Vendor Class
  > Option Request
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6
Expression… + IPv6_RA IPv6_RS icmpv6-dhcpv6 dhcpv6
Packets: 2707 · Displayed: 1134 (41.7%) · Load time: 0:0.46
Profile: IPv6

SharkFest'23 US
San Diego, CA – June 10-15

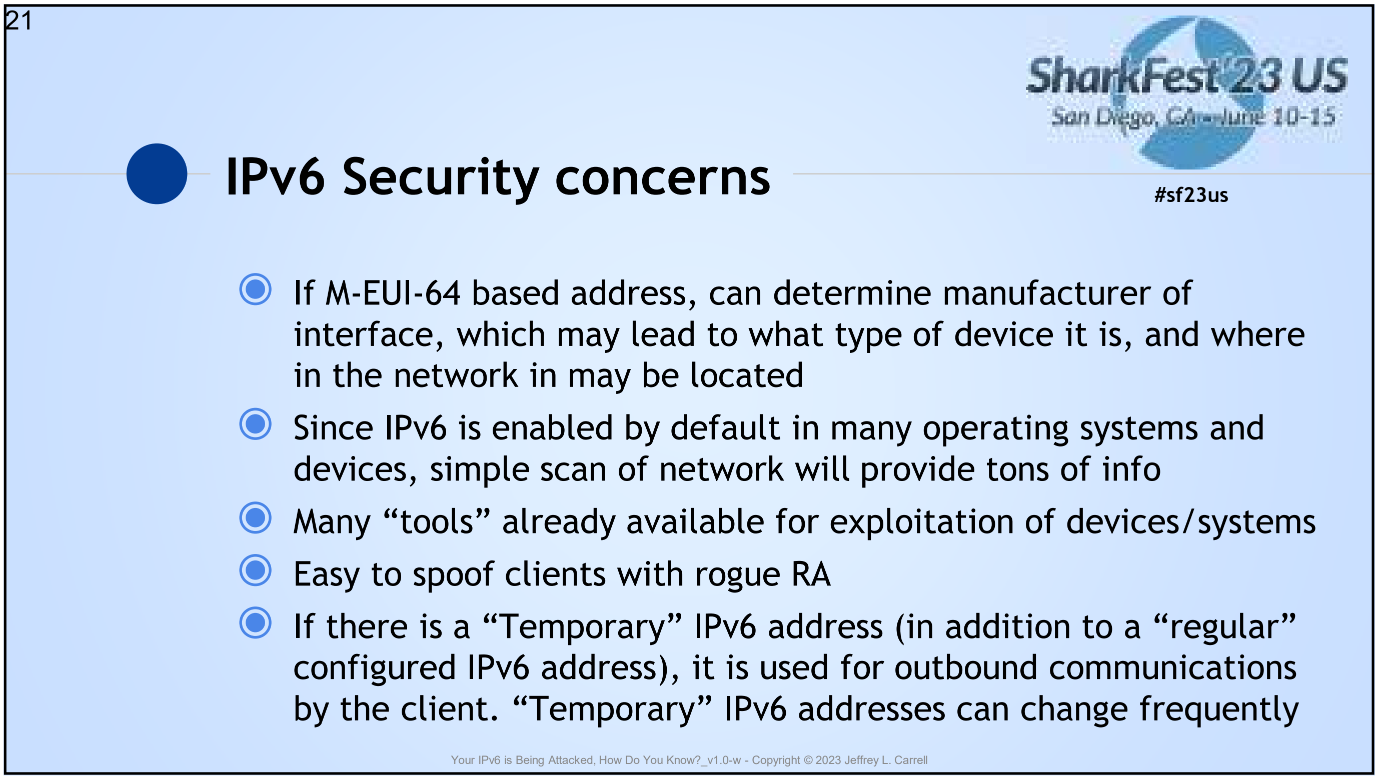
Nested display filter buttons

#sf23us



```
No.    Delta  Time  Source                     Destination  Protocol  Length
46445  0      201…  fe80::958c:8d52:57d:fe80   ff02::1:3              84
46447  0      201…  fe80::958c:8d52:57d:fe80   ff02::1:3              84
46449  0      201…  fe80::958c:8d52:57d:fe80   ff02::1:3              84
46467  2      201…  fe80::f252                 ff02::5      OSPF      90
46493  8      201…  fe80::20c:29ff:fe02:5f8c   ff02::1      ICMPv6    110
46497  1      201…  fe80::f252                 ff02::5      OSPF      90
```

2_IPv6-in-Wireshark_Feb2017.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6
+ IPv6 IPv6-router-traffic IPv6-I
IPv6_RS
IPv6_RA
IPV6_RS-RA
2_IPv6-in-Wireshark_Feb2017.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ipv6
+ IPv6 IPv6-router-traffic IPv6-DHCPv6 IPv6-addr icmpv6-dhcpv6 IPv6_DAD pkt_comment
No. Delta Time Source Destination Protocol Length Info
Ethernet

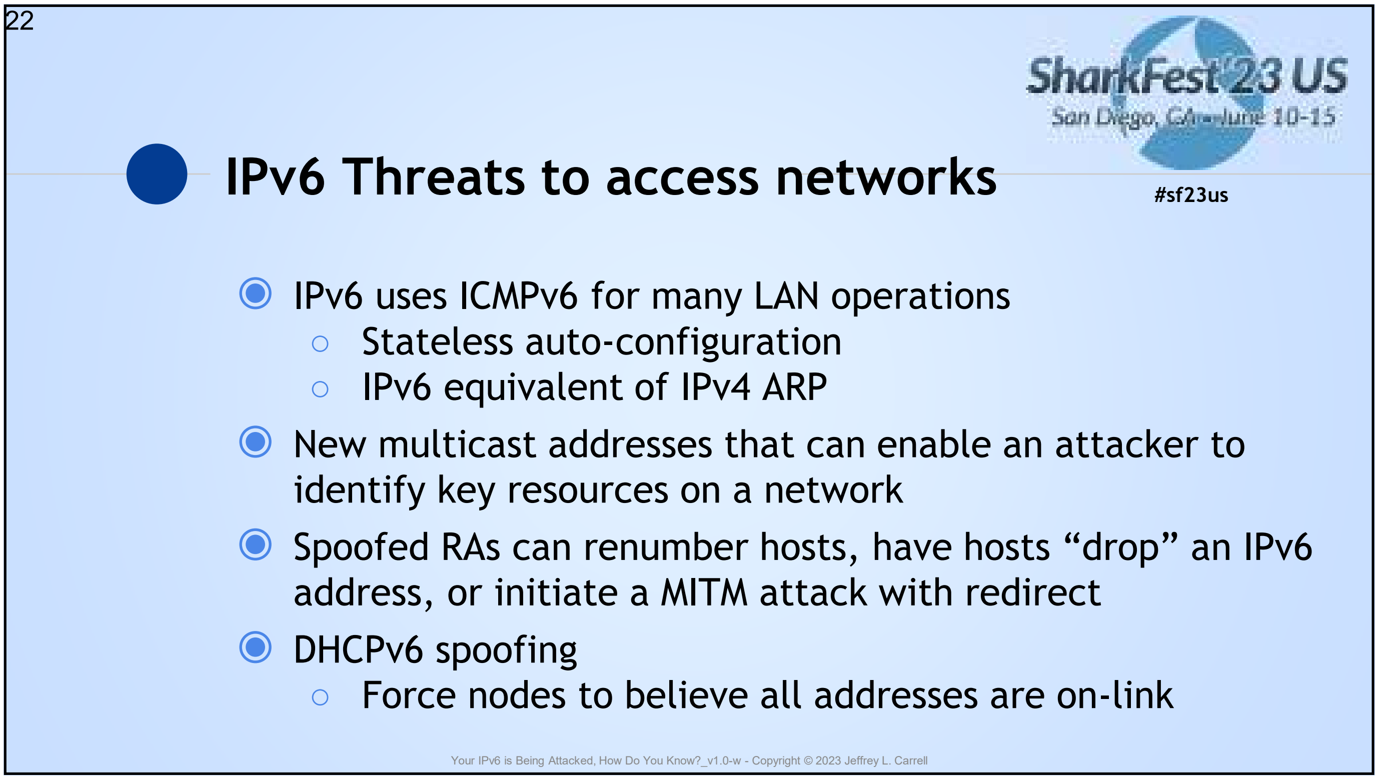


21

SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

IPv6 Security concerns

- If M-EUI-64 based address, can determine manufacturer of interface, which may lead to what type of device it is, and where in the network in may be located
- Since IPv6 is enabled by default in many operating systems and devices, simple scan of network will provide tons of info
- Many “tools” already available for exploitation of devices/systems
- Easy to spoof clients with rogue RA
- If there is a “Temporary” IPv6 address (in addition to a “regular” configured IPv6 address), it is used for outbound communications by the client. “Temporary” IPv6 addresses can change frequently

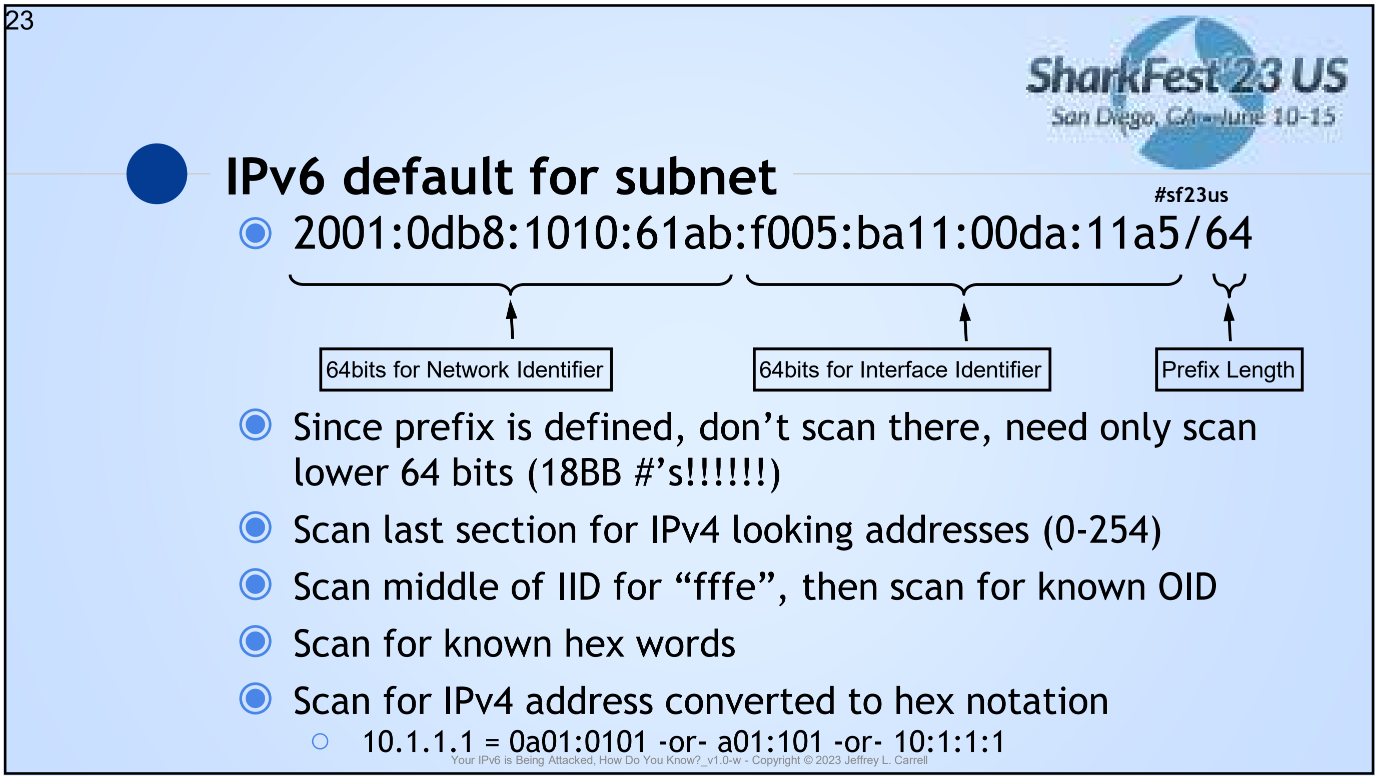


22

SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

IPv6 Threats to access networks

- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent of IPv4 ARP
- New multicast addresses that can enable an attacker to identify key resources on a network
- Spoofed RAs can renumber hosts, have hosts “drop” an IPv6 address, or initiate a MITM attack with redirect
- DHCPv6 spoofing
  - Force nodes to believe all addresses are on-link



23

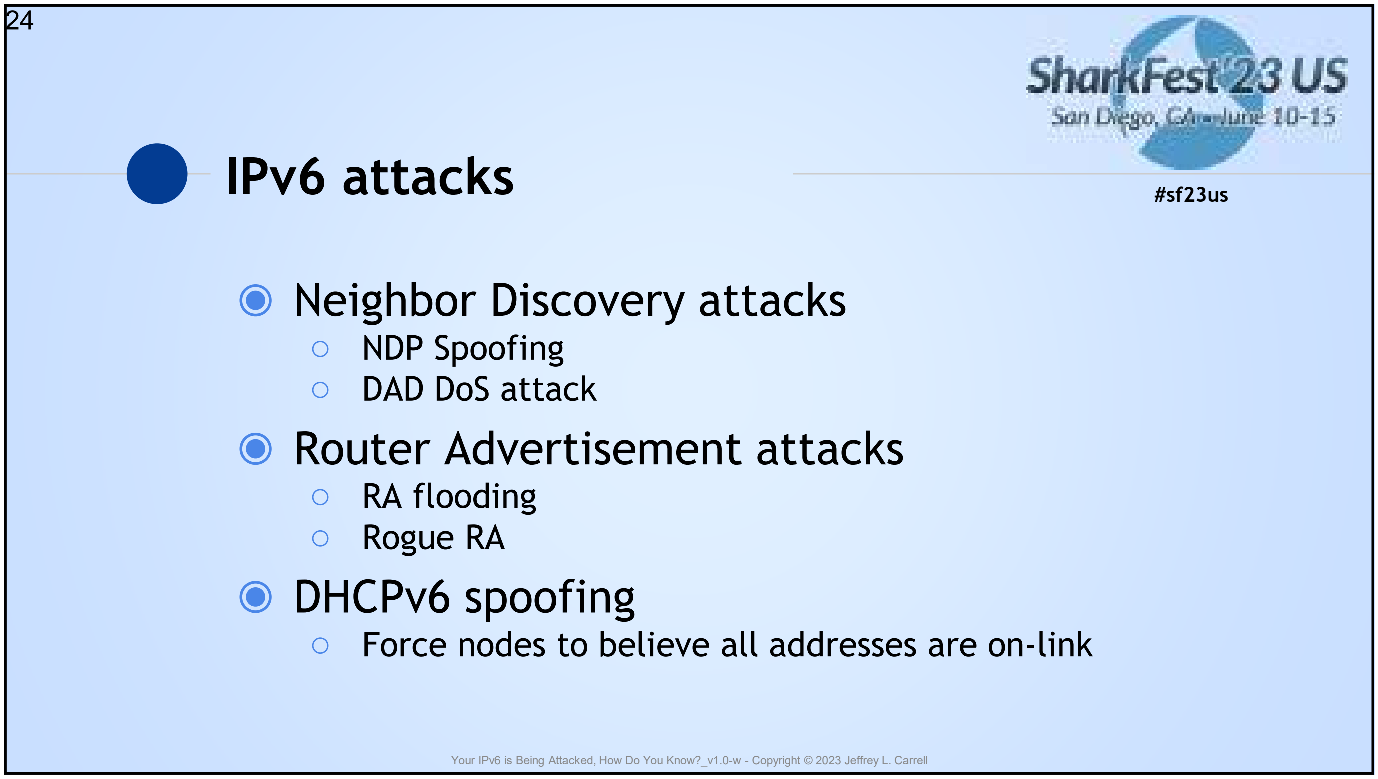
SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

IPv6 default for subnet

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

64bits for Network Identifier
64bits for Interface Identifier
Prefix Length

- Since prefix is defined, don’t scan there, need only scan lower 64 bits (18BB #’s!!!!!!)
- Scan last section for IPv4 looking addresses (0-254)
- Scan middle of IID for “fffe”, then scan for known OID
- Scan for known hex words
- Scan for IPv4 address converted to hex notation
  - 10.1.1.1 = 0a01:0101 -or- a01:101 -or- 10:1:1:1



24

SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

IPv6 attacks

- Neighbor Discovery attacks
  - NDP Spoofing
  - DAD DoS attack
- Router Advertisement attacks
  - RA flooding
  - Rogue RA
- DHCPv6 spoofing
  - Force nodes to believe all addresses are on-link

25

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

IPv6 Attack tools

- Attack Toolkits
  - THC-IPv6
    - https://github.com/vanhauser-thc/thc-ipv6
  - SI6 Networks IPv6 Toolkit
    - https://github.com/fgont/ipv6toolkit
- Scanners
  - Nmap, halfscan6 (older)
- Packet forgery
  - Scapy
  - Chiron

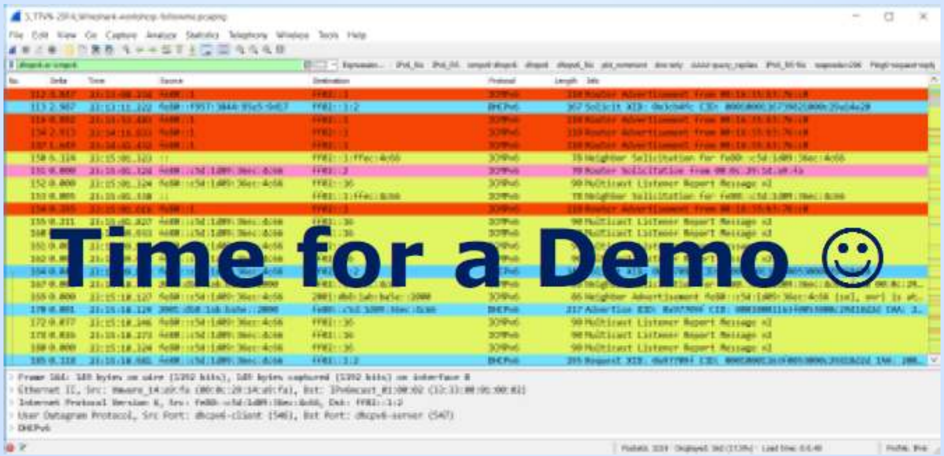
Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

26

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Wireshark demo #1 - watch me



Time for a Demo ☺

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

27

https://github.com/jeffcarrell/Sharkfest19-US--IPv6-Troubleshooting-with-Wireshark

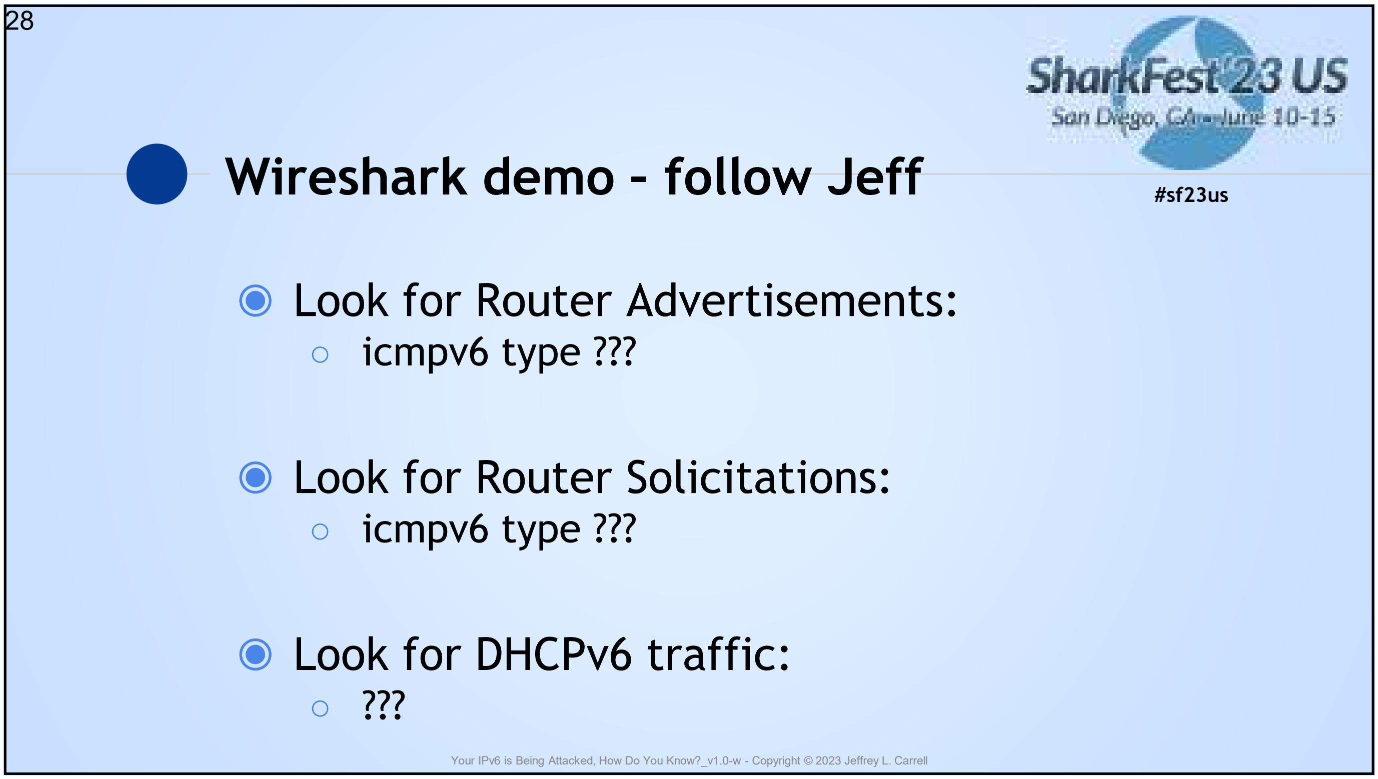
SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

IPv6 in Wireshark - follow Jeff

- Open: “1_IPv6-in-Wireshark_Feb2017.pcapng”
- Let’s look at the trace from the “default” configuration profile and from a custom profile called “IPv6”
- Now let’s view some IPv6 specifics, we’ll create some display filters to help

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell



28

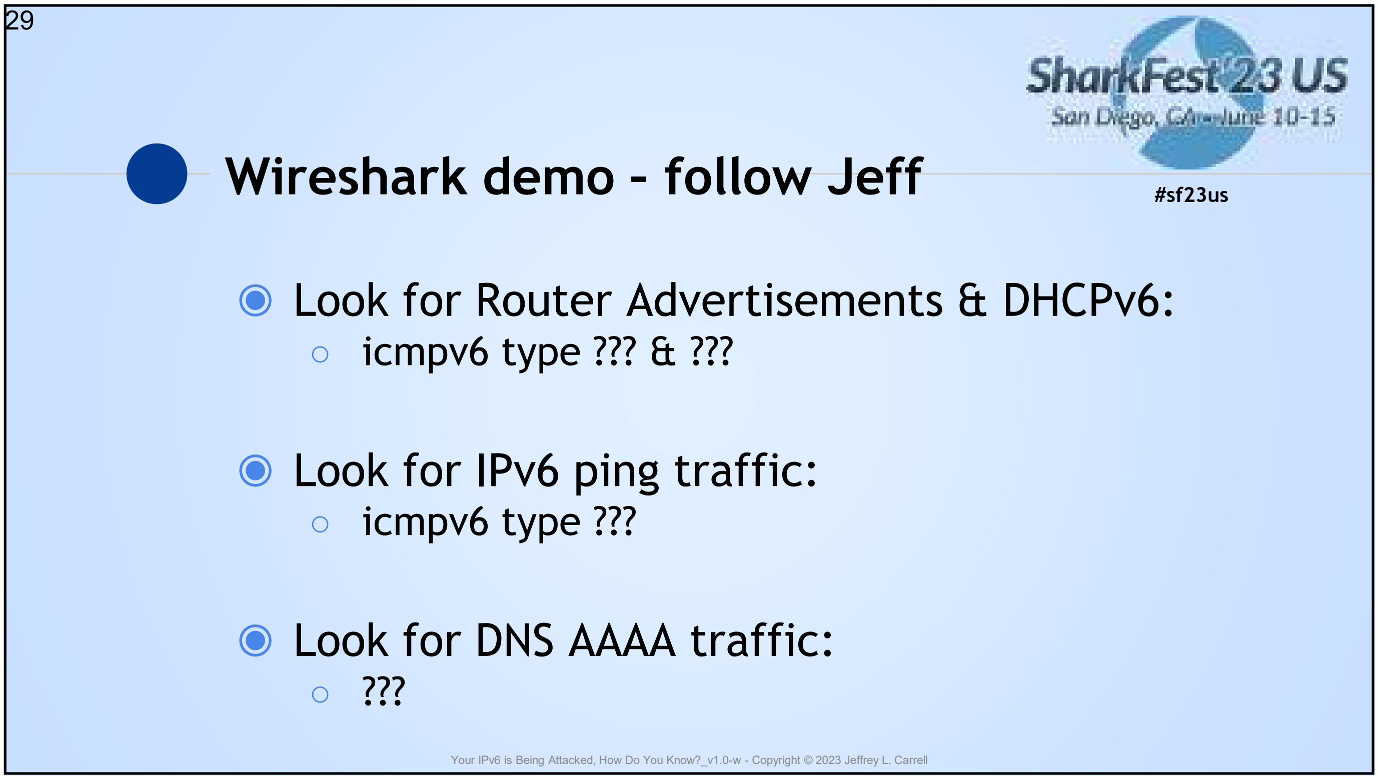
SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

Wireshark demo - follow Jeff

- Look for Router Advertisements:
  - icmpv6 type ???
- Look for Router Solicitations:
  - icmpv6 type ???
- Look for DHCPv6 traffic:
  - ???

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell



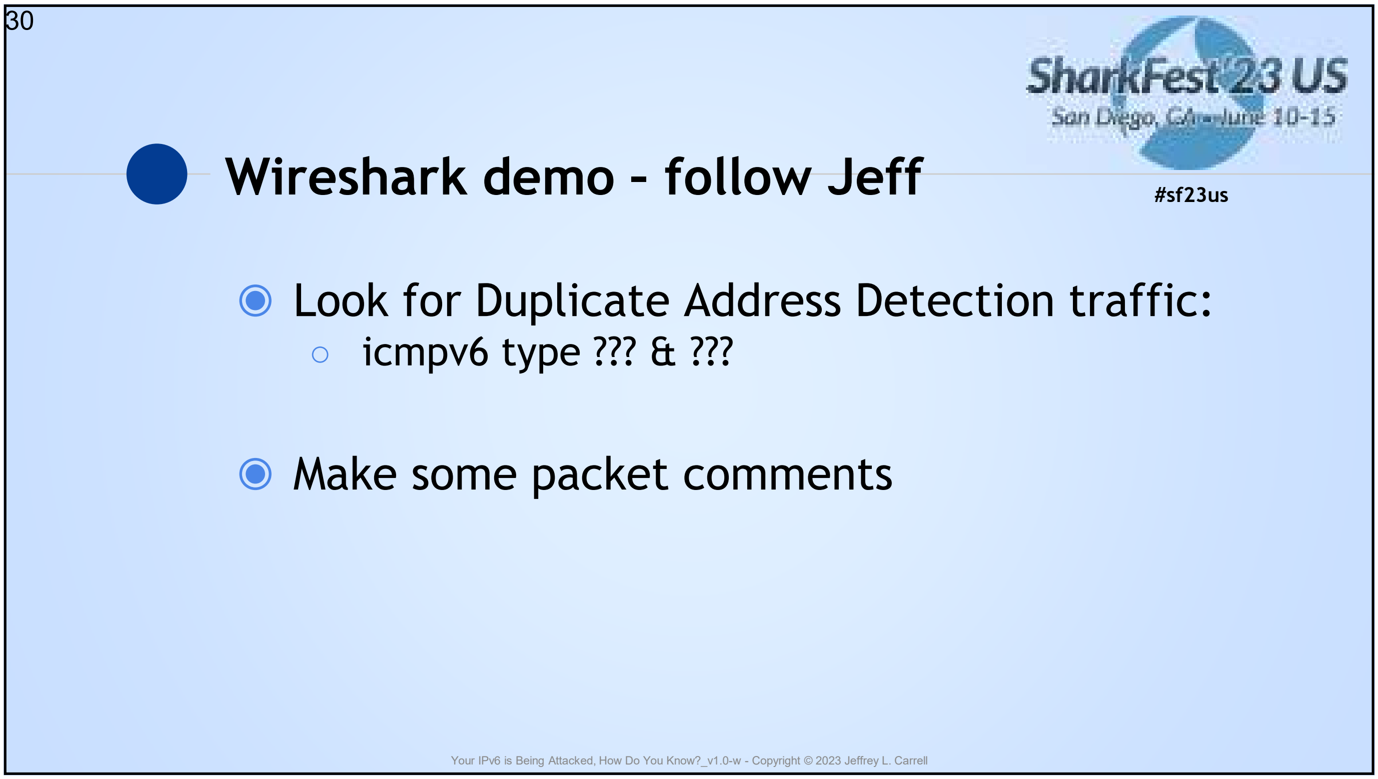
29

SharkFest'23 US
San Diego, CA - June 10-15
#sf23us

Wireshark demo - follow Jeff

- Look for Router Advertisements & DHCPv6:
  - icmpv6 type ??? & ???
- Look for IPv6 ping traffic:
  - icmpv6 type ???
- Look for DNS AAAA traffic:
  - ???

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell



30

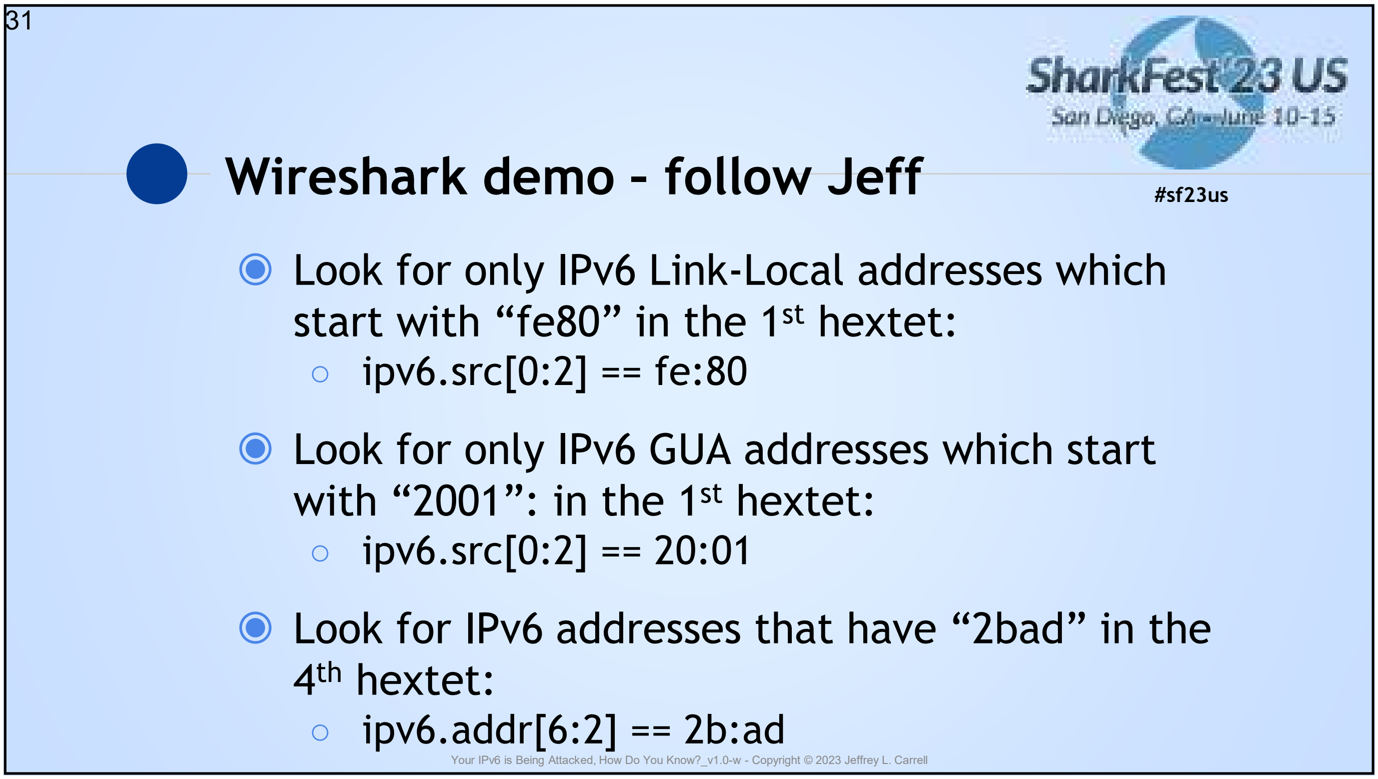
SharkFest'23 US
San Diego, CA - June 10-15
#sf23us

Wireshark demo - follow Jeff

- Look for Duplicate Address Detection traffic:
  - icmpv6 type ??? & ???
- Make some packet comments

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

31

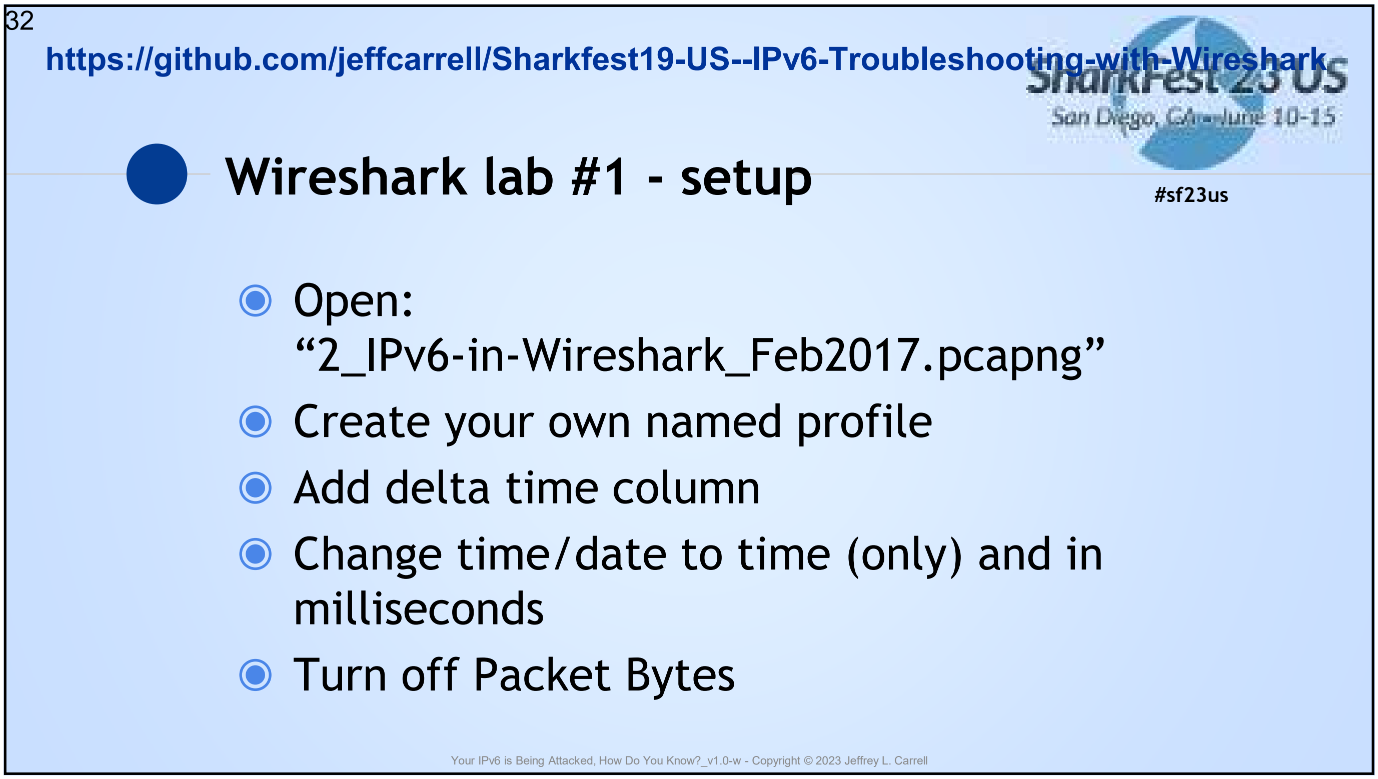


SharkFest'23 US
San Diego, CA - June 10-15
#sf23us

Wireshark demo - follow Jeff

- Look for only IPv6 Link-Local addresses which start with "fe80" in the 1st hextet:
  - ipv6.src[0:2] == fe:80
- Look for only IPv6 GUA addresses which start with "2001": in the 1st hextet:
  - ipv6.src[0:2] == 20:01
- Look for IPv6 addresses that have "2bad" in the 4th hextet:
  - ipv6.addr[6:2] == 2b:ad

32

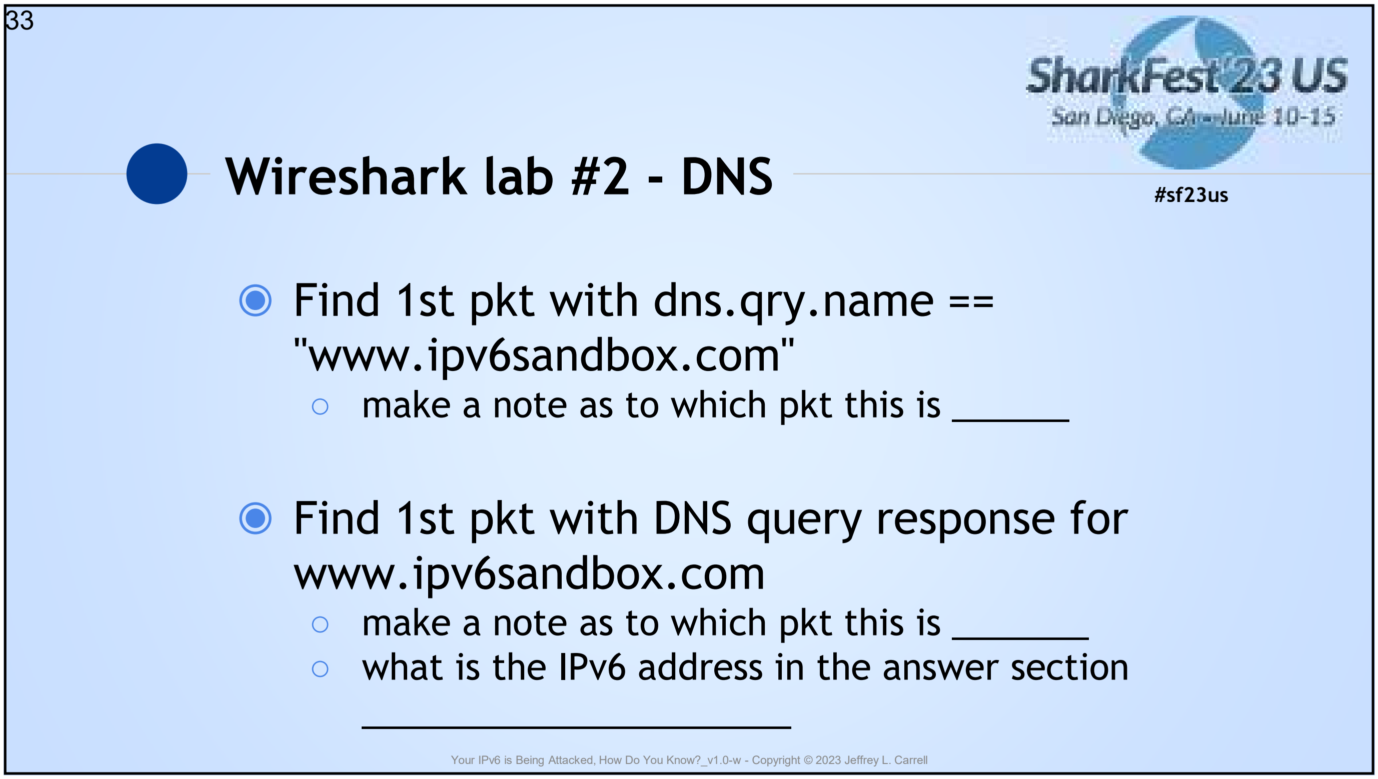


https://github.com/jeffcarrell/Sharkfest19-US--IPv6-Troubleshooting-with-Wireshark

SharkFest'23 US
San Diego, CA - June 10-15
#sf23us

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



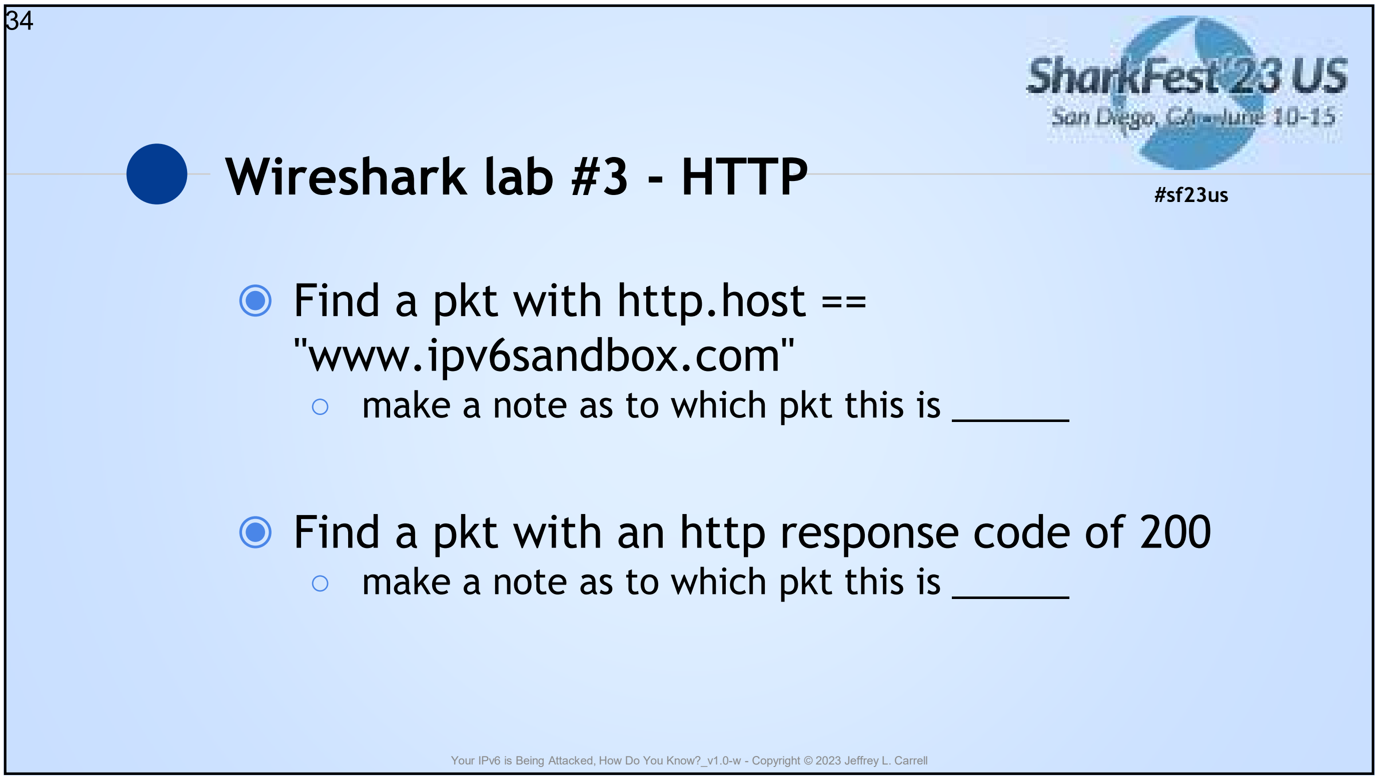
33

SharkFest'23 US
San Diego, CA - June 10-15
#sf23us

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

    ____

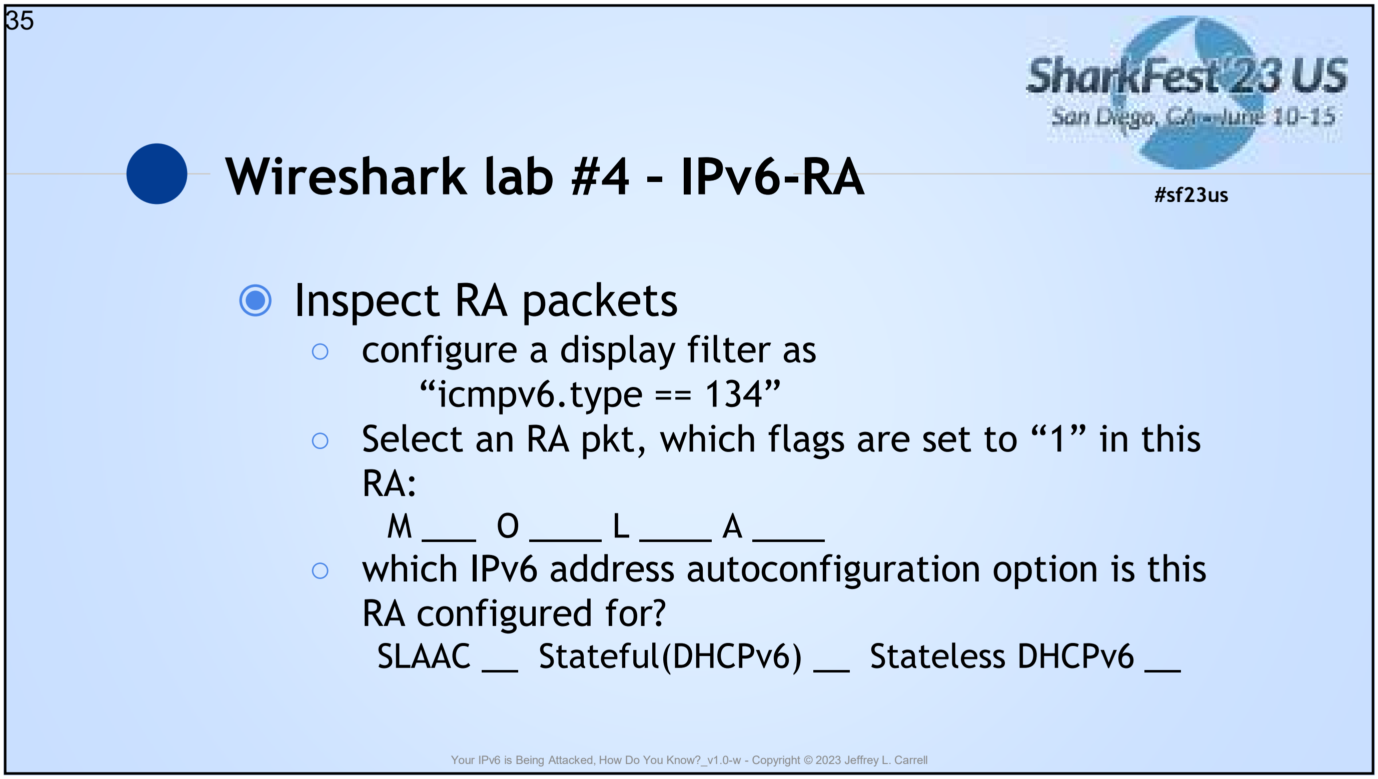


34

SharkFest'23 US
San Diego, CA - June 10-15
#sf23us

Wireshark lab #3 - HTTP

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

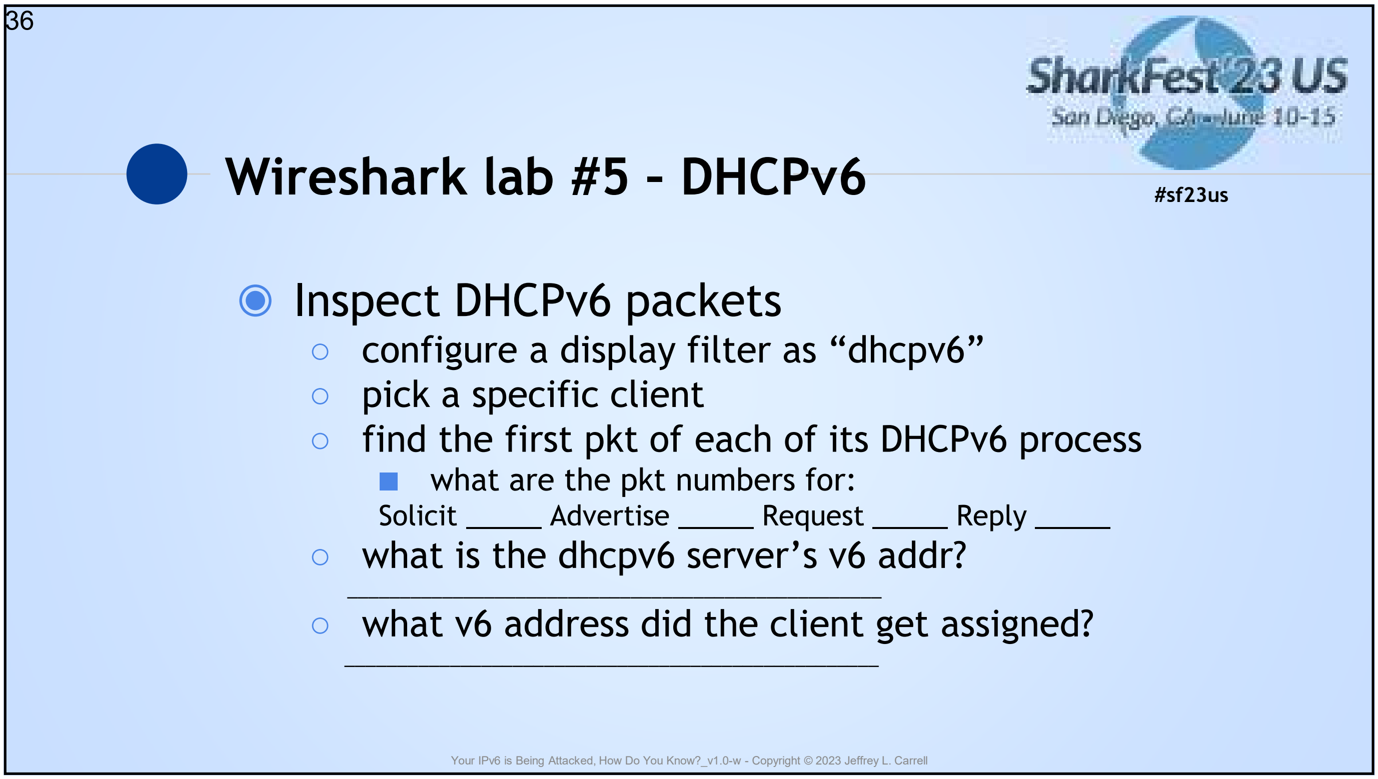


35

#sf23us

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" in this RA:
    M ___ O ____ L ____ A ____
  - which IPv6 address autoconfiguration option is this RA configured for?
    SLAAC __ Stateful(DHCPv6) __ Stateless DHCPv6 __

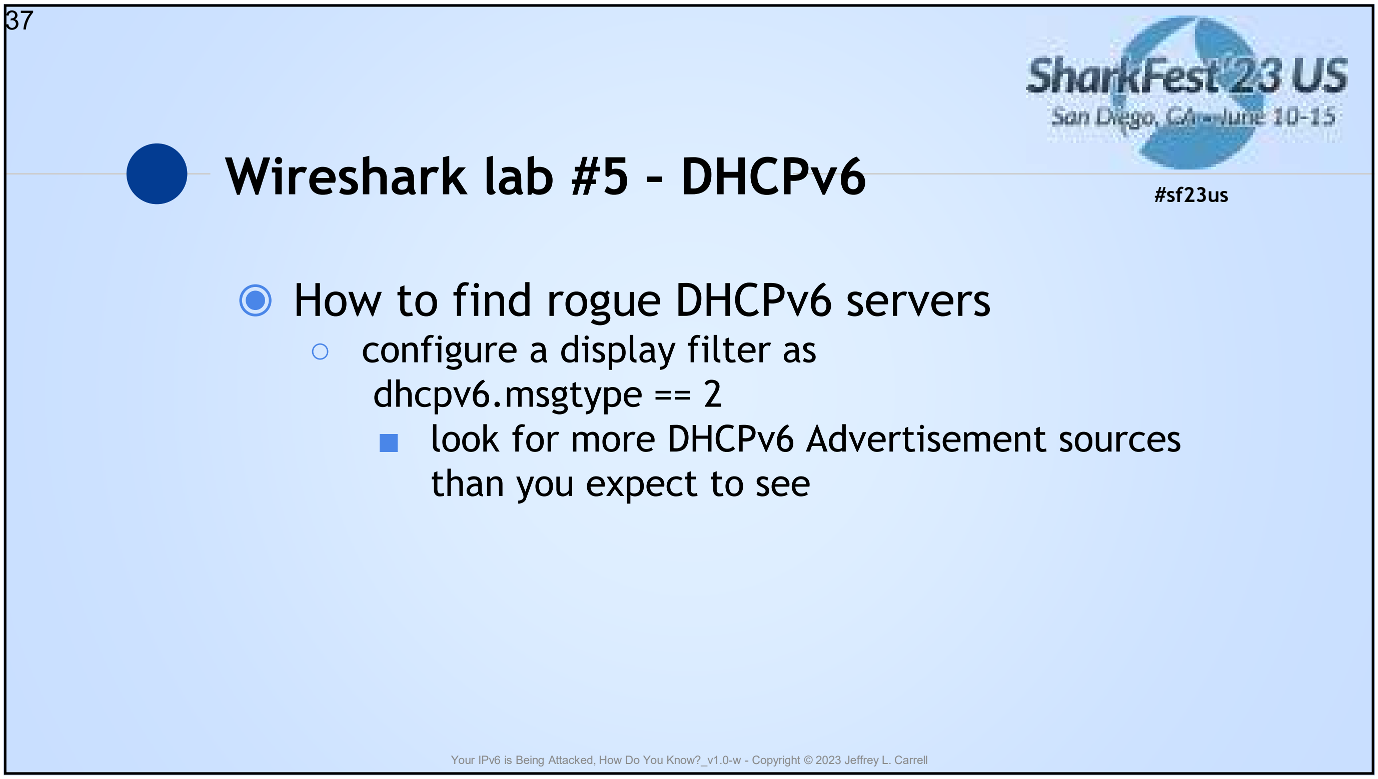


36

#sf23us

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?
    ____



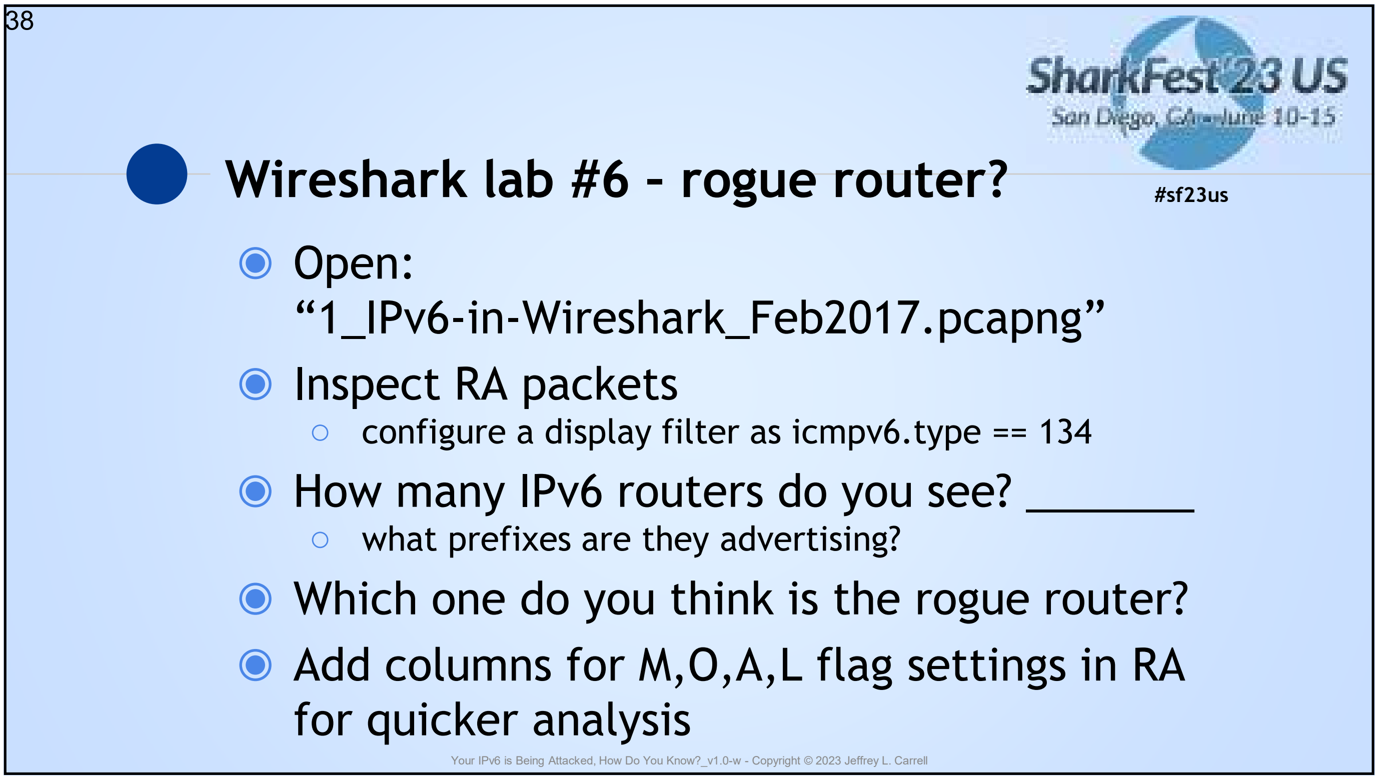
37

SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

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



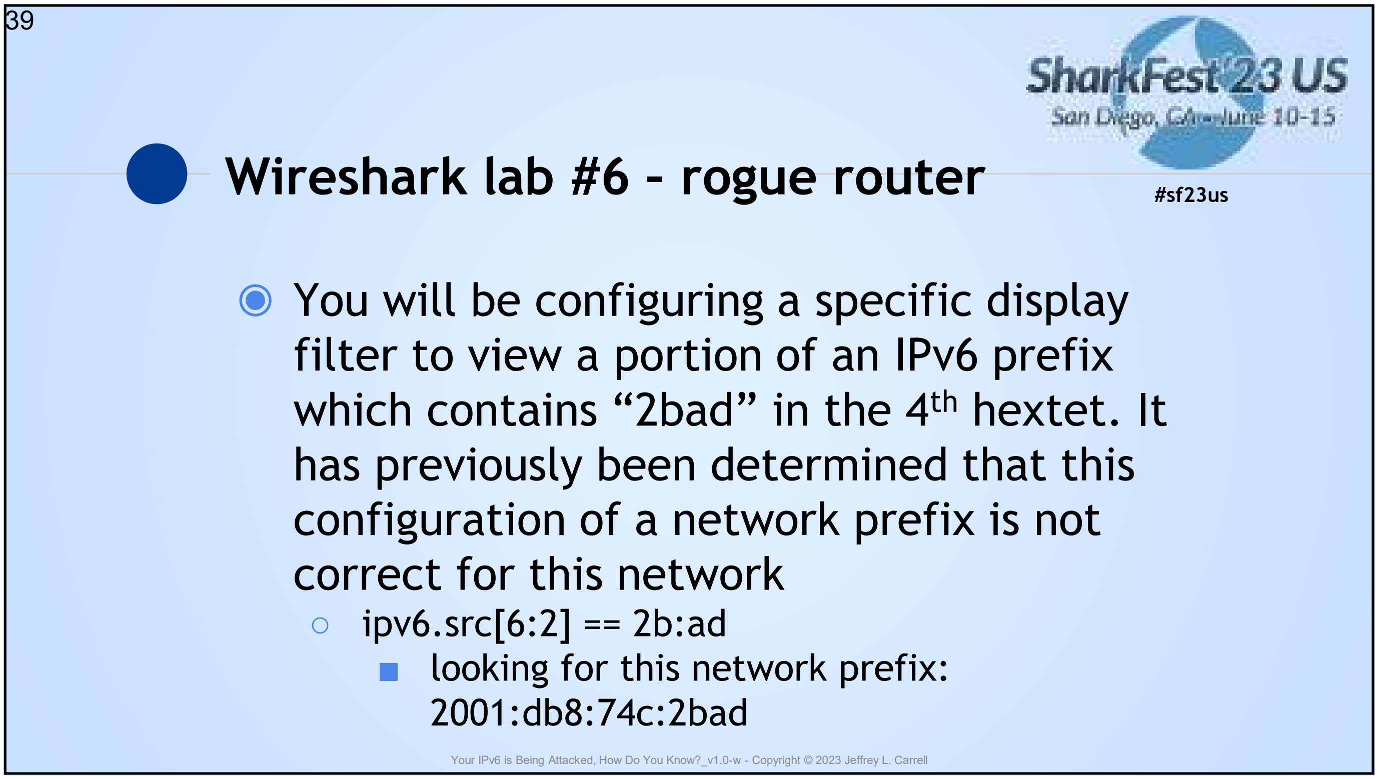
38

SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

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 the rogue router?
- Add columns for M,O,A,L flag settings in RA for quicker analysis

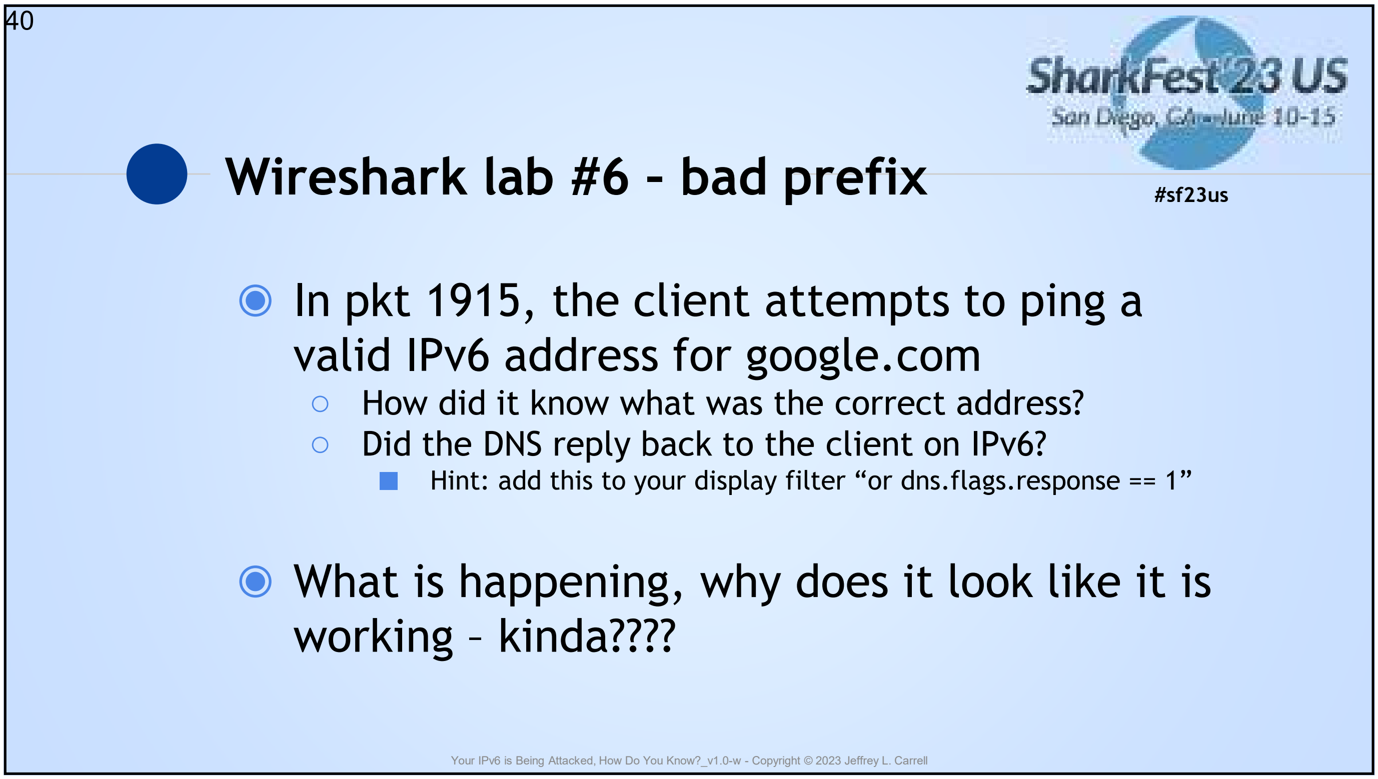


39

SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

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
    - looking for this network prefix: 2001:db8:74c:2bad



40

SharkFest'23 US
San Diego, CA – June 10-15
#sf23us

Wireshark lab #6 - bad prefix

- In pkt 1915, the client attempts to ping a valid IPv6 address for google.com
  - How did it know what was the correct address?
  - Did the DNS reply back to the client on IPv6?
    - Hint: add this to your display filter “or dns.flags.response == 1”
- What is happening, why does it look like it is working – kinda????

41

Wireshark lab #7 - did you see that

#sf23us

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

42

Wireshark lab #8 - lots of prefixes

#sf23us

- 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?

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

SharkFest'23 US
San Diego, CA • June 10-15

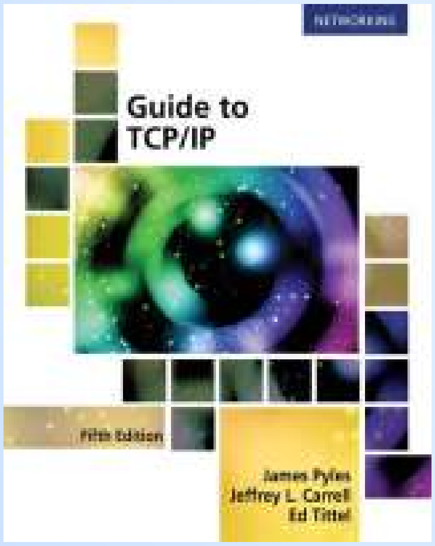
#sf23us

IPv6 Essentials Reference Sheet

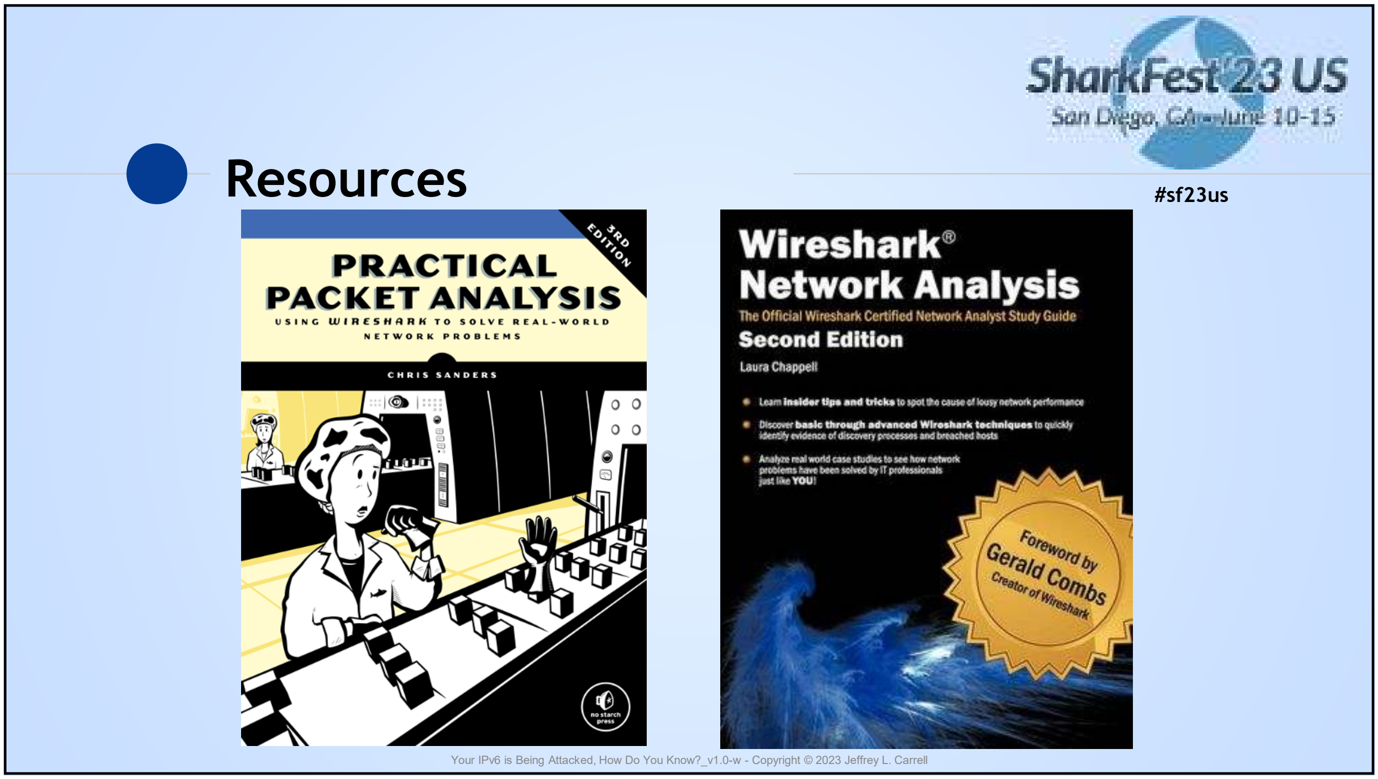
SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Resources



cisco
SECURITY
IPv6 Security
Information assurance for the next-generation Internet Protocol
Scott Hogg
Eric Vyncke



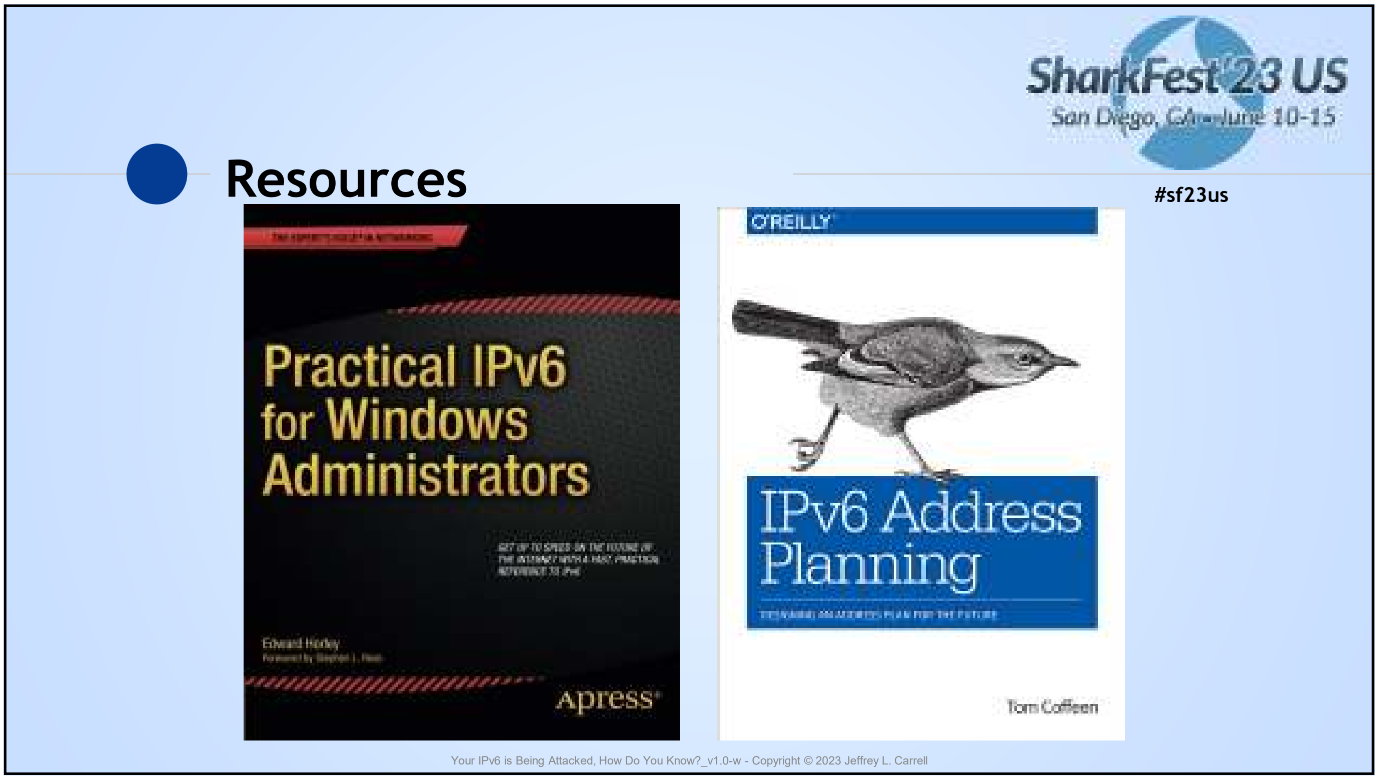
SharkFest'23 US
San Diego, CA – June 10-15

Resources

#sf23us

3RD EDITION
PRACTICAL PACKET ANALYSIS
USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS
CHRIS SANDERS
no starch press
Wireshark® Network Analysis
The Official Wireshark Certified Network Analyst Study Guide
Second Edition
Laura Chappell
Learn insider tips and tricks to spot the cause of lousy network performance
Discover basic through advanced Wireshark techniques to quickly identify evidence of discovery processes and breached hosts
Analyze real world case studies to see how network problems have been solved by IT professionals just like YOU!
Foreword by Gerald Combs Creator of Wireshark

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell



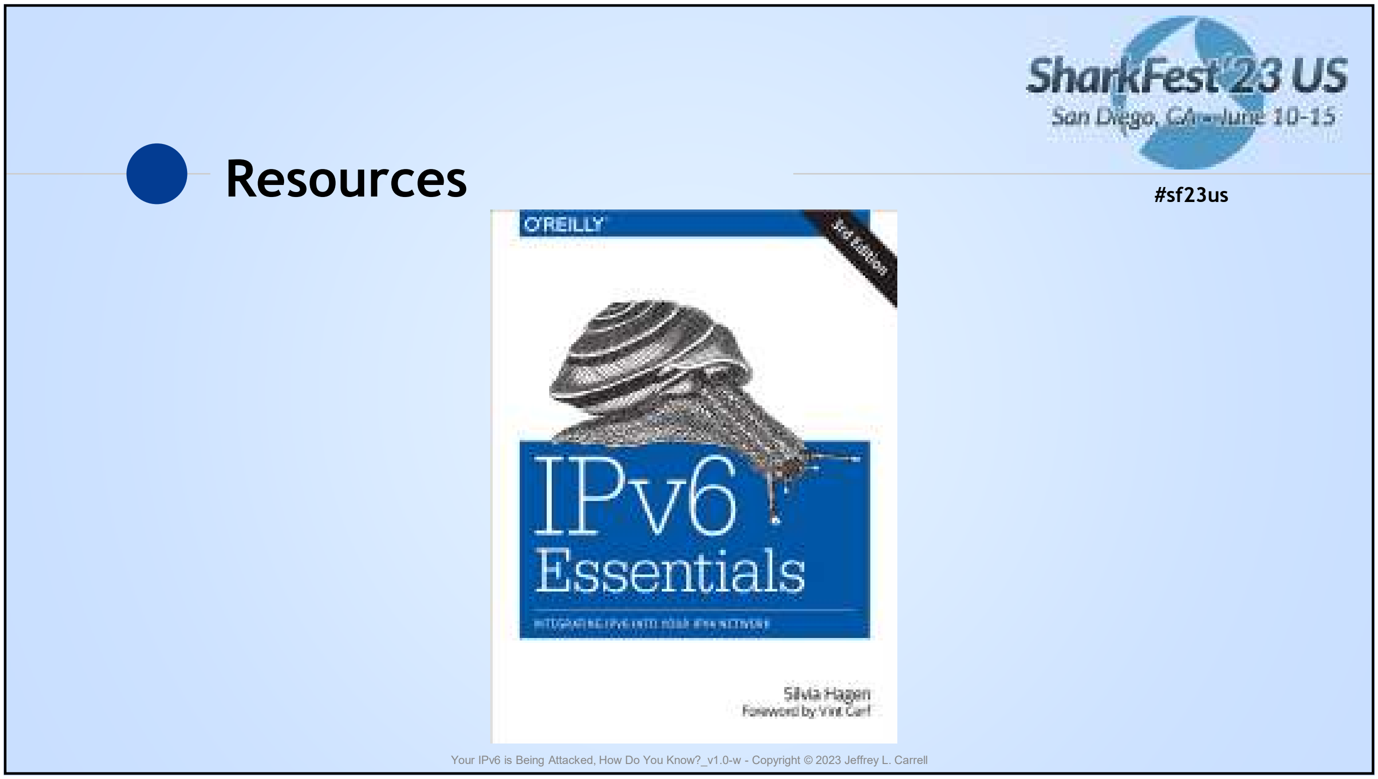
SharkFest'23 US
San Diego, CA – June 10-15

Resources

#sf23us

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
Apress®
O'REILLY®
IPv6 Address Planning
DESIGNING AN ADDRESS PLAN FOR THE FUTURE
Tom Coffeen

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell



SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Resources

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Resources

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell

SharkFest'23 US
San Diego, CA – June 10-15

#sf23us

Thank You for Attending!

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

IPv6 FORUM CERTIFIED ENGINEER
IPv6 FORUM CERTIFIED TRAINER

Certificate of Completion
jeffcarrell
hereby attained the rank of
Sage
Hurricane Electric
IPv6 Certification

Your IPv6 is Being Attacked, How Do You Know?_v1.0-w - Copyright © 2023 Jeffrey L. Carrell