imnurnet – Exploiting Your IPv4 Network with IPv6

Jeffrey L Carrell
Master Technologist
HPE Services, Education
Hewlett Packard Enterprise

Networking, Container and Data Analytics technologies
Instructor/Course Developer

jeff.carrell@teachmeipv6.com
X – fna Twitter: @JeffCarrell_v6

#sf25us

1

Monday, just another day…

- it's 0800hrs on a Monday, morning crowd shuffles in
  - at anycompany.com
- red team walks in, starts an NMAP ping scan
  - to see if blue team is awake
- blue team, drinking coffee, sees an alert that detects a ping scan
  - "hahahaha, caught you red team"
- network team, drinking a higher caffeinated drink, says "it was DNS“
  - obviously someone else's problem, cause it's never the network
- server team, eating morning pastry, says "it was the network,
  - cause our servers never cause problems"
- desktop team <snoring lightly>, wakes, sputters "who we talking about?"
- applications team, sipping lattes, pushes to production first thing in the morning
  - "cause everyone is here if there are problems, not that we expect any"
- meanwhile, at an undisclosed location
  - a windowless building, lots of fiber and power coming in
- blackhatbubba is running an AI bot, finds an open port
  - bwa-hahahaha, gotcha anycompany.com

2

Legal bits

- I work for HPE, this not an HPE presentation and I am not here on behalf of HPE
- The TXv6TF sponsored my being here with y'all. I am a board member of this non-profit group
- The system I am accessing and exploiting is owned completely by me and is not a production system
- DO NOT attempt these types of activities without WRITTEN approvals
- …and of course, the packets never lie…

imnurnet – Exploiting Your IPv4 Network with IPv6

- IPv6 – a few fundamentals
- Wireshark color rules & display filters
- imnurnet recon/exploit of an "IPv4 only" network using IPv6

IPv6 default for subnet

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

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

Address types

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

Address scopes

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

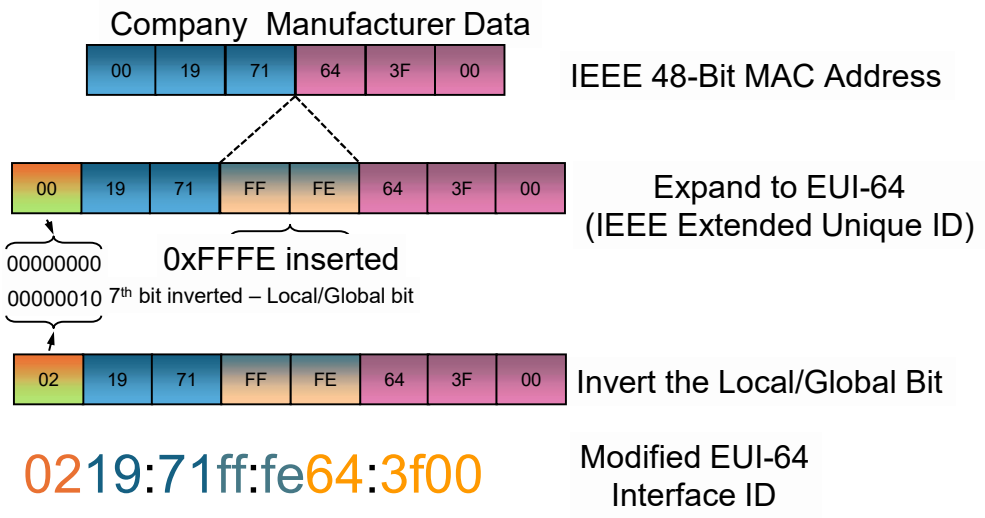
IPv4/IPv6 special addresses

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

IPv6 well known multicast addresses

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

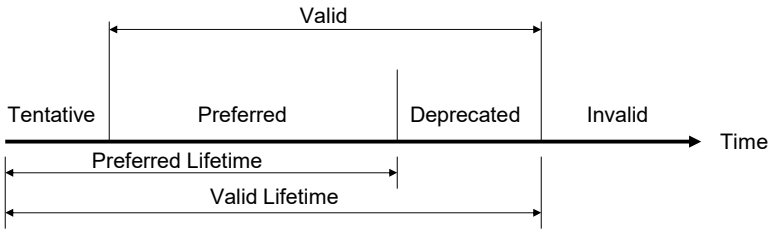
Interface ID from MAC address



Interface ID from Random Number

- RFC4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- Initial IID is derived based on mathematical computation to create a "random 64bit number" and appended to prefix to create a GUA
- An additional but different 64bit number is computed, appended to prefix, and tagged "temporary" for a 2nd GUA
- Temporary GUA should be re-computed on a frequent basis
- Temporary GUA is used as primary address for communications, as it is considered "more secure"

Lifetime states of an IPv6 address



- Tentative – address is in process of verification for uniqueness and is not yet available for regular communications
- Valid – address is valid for use in communication based on Preferred and Deprecated status
- Preferred – address is usable for all communications
- Deprecated – address can still be used for existing sessions, but not for new sessions
- Invalid – an address is no longer available for sending or receiving

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)

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 autoconfiguration options

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

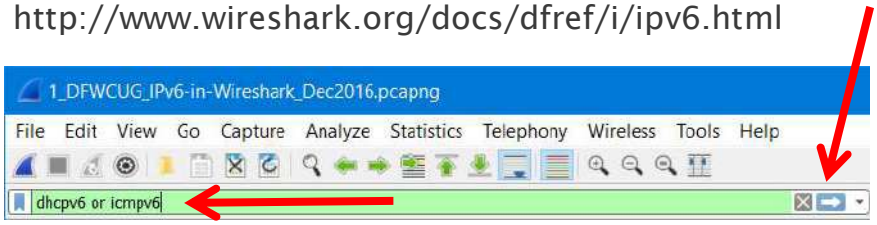
Coloring rules

1710	0.062	17:46:18.096	fe80::5	fe80::68ec:6151:8d5f:2da2	ICMPv6	86 Neighbor Solicitation for fe80::68ec:6…
1711	0.000	17:46:18.096	fe80::68ec:6151:8d5f:2da2	fe80::5	ICMPv6	86 Neighbor Advertisement fe80::68ec:6151…
1712	1.158	17:46:19.255	10.105.2.100	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1713	2.241	17:46:21.496	fe80::5	ff02::5	OSPF	90 Hello Packet
1714	0.699	17:46:22.196	10.105.2.1	224.0.0.5	OSPF	78 Hello Packet
1715	0.058	17:46:22.255	10.105.2.100	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1716	9.641	17:46:31.896	fe80::5	ff02::5	OSPF	90 Hello Packet
1717	0.299	17:46:32.196	10.105.2.1	224.0.0.5	OSPF	78 Hello Packet
1718	3.268	17:46:35.464	fe80::68ec:6151:8d5f:2da2	ff02::1:2	DHCPv6	152 Solicit XID: 0x99ae2a CID: 0001000115e…
1719	0.004	17:46:35.468	fe80::20c:29ff:febb:6265	fe80::68ec:6151:8d5f:2da2	DHCPv6	166 Advertise XID: 0x99ae2a CID: 000100011…
1720	0.003	17:46:35.472	fe80::5	fe80::68ec:6151:8d5f:2da2	DHCPv6	184 Advertise XID: 0x99ae2a CID: 000100011…
1721	0.470	17:46:35.942	fe80::68ec:6151:8d5f:2da2	ff02::2	ICMPv6	70 Router Solicitation from 00:1c:14:82:0…
1722	0.000	17:46:35.943	fe80::5	ff02::1	ICMPv6	118 Router Advertisement from 00:24:38:ee:…
1723	0.278	17:46:36.221	BrocadeC_ee:ea:c3	LLDP_Multicast	LLDP	133 TTL = 120 System Name = group05_NetIron
1724	0.237	17:46:36.458	fe80::68ec:6151:8d5f:2da2	ff02::1:2	DHCPv6	198 Request XID: 0x99ae2a CID: 0001000115e…
1725	0.001	17:46:36.459	fe80::20c:29ff:febb:6265	fe80::68ec:6151:8d5f:2da2	DHCPv6	166 Reply XID: 0x99ae2a CID: 0001000115e87…
1726	0.005	17:46:36.464	fe80::68ec:6151:8d5f:2da2	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
1727	0.005	17:46:36.469	fe80::68ec:6151:8d5f:2da2	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
1728	0.000	17:46:36.470	10.105.2.100	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0.…

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

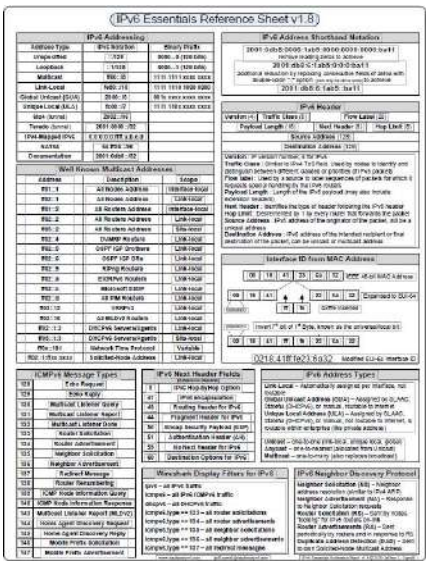
Using Wireshark to view IPv6 pkts

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

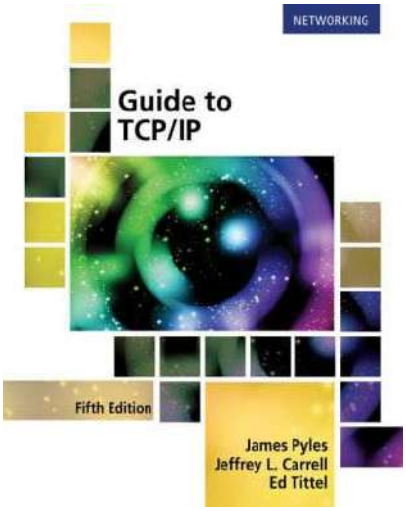


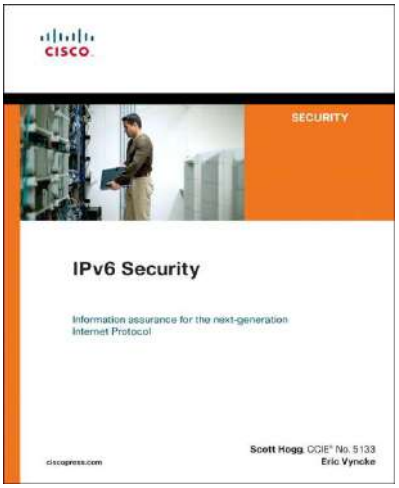
IPv6 Essentials Reference Sheet

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

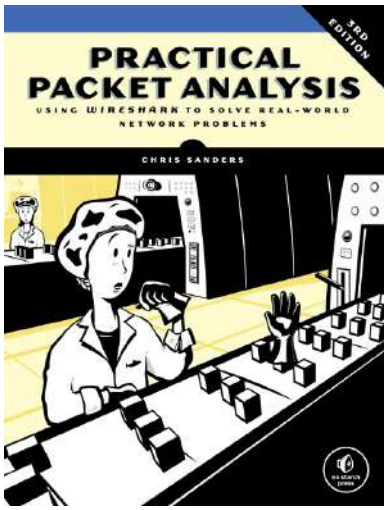


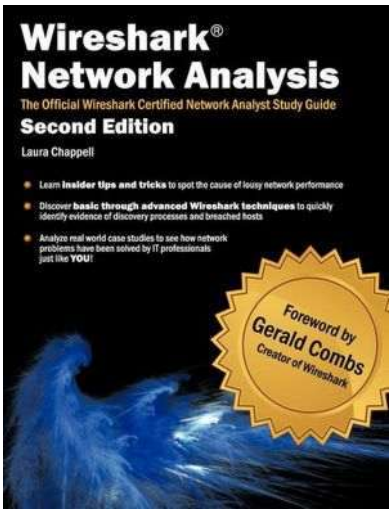
Resources



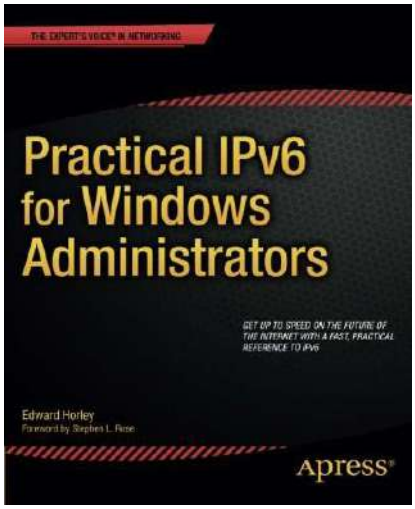


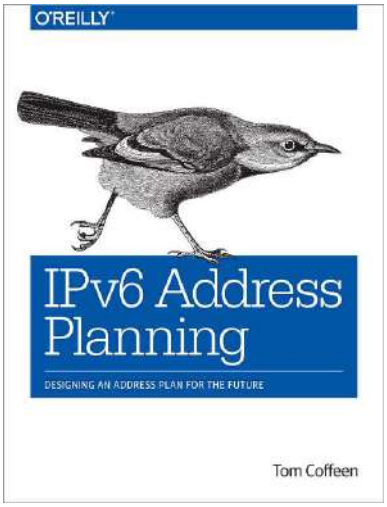
Resources



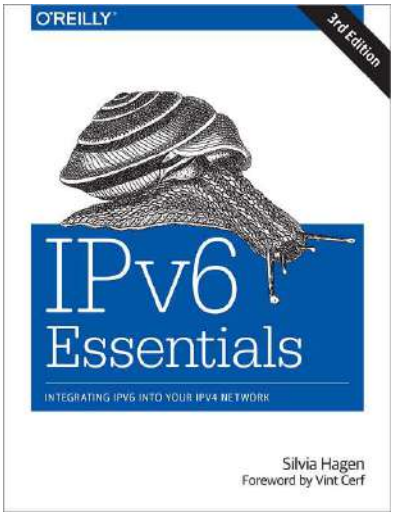


Resources

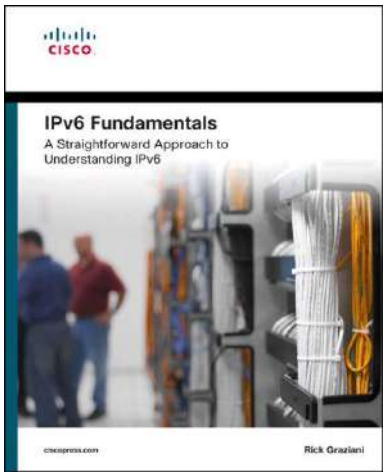


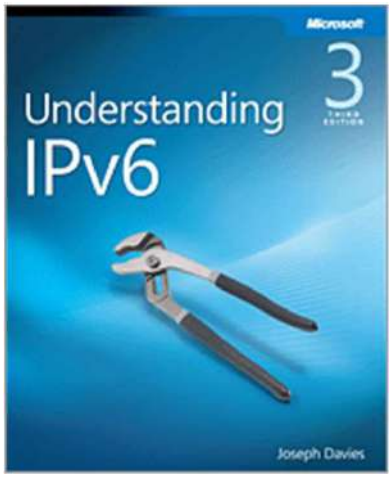


Resources



Resources





Imnurnet demo

recon/exploit of an "IPv4 only" network using IPv6

Disclaimer

DO NOT execute these security assessment tools on a network without proper authorization !!

imnurnet

- Find an exploitable system via IPv4 (target)
- Create a new admin account on target
- Download some apps and iso's on target:
  - Wireshark, VirtualBox, Wireless Network Watcher
  - VyOS, Ubuntu, THC-IPv6
- Create IPv6 router VM for internal net, will allow local nodes to acquire IPv6 addresses
- Create Linux client VMs for infiltrating and recon of internal network via IPv6
- Use Wireshark to find internal nodes via IPv6
- Commandeer internal nodes via IPv6 for additional recon

Thank You for Attending!

jeff.carrell@teachmeipv6.com

Twitter: @JeffCarrell_v6