IPv6 Cheatsheet

IPv6 Protocol header (RFC2460)

+-+-+-+-+-	+-+-+-	+-+-+-++	-+-+-	-+-+-	+-+-+	+-+-+-	-+-+-	+-+-+	-+-+
Version	Traffic	Class		Flow	Label				1
+-+-+-+-+-	+-+-+-	+-+-+-++	-+-+-	-+-+-	+-+-+	+-+-+-	-+-+-	+-+-+	-+-+
1	Payload	Length	1	Next	Header	1	Нор	Limit	1
+-+-+-+-	+-+-+-	+-+-+-+	-+-+-	-+-+-	+-+-+	+ - + - + -	-+-+-	+-+-+	-+-+
1									1
+									+
1									1
+		Sou	rce Ad	dress	5				+
1									1
+									+
1									1
+-+-+-+-	+-+-+-	+-+-+-+	-+-+-	-+-+-	+-+-+	+ - + - + -	+-+-	+-+-+	-+-+
1									1
+									+
1									1
+		Destin	ation A	Addre	ss				+
1									1
+									+
1									1

Version(4-bit) Always set to 6 Traffic Class(8-bit) A DSCP value for QoS Flow Label(20-bit) Identifies unique flows Payload Length(16-bit) Length of the payload in bytes Next Header(8-bit) Header or protocol which follows Hop Limit (8-bits) Similar to IPv4's time to live field Source Address (128-bit) Source IP address Destination Address(128-bit)Dest. IP addresses

Extension Headers (RFC2460)

+++++++	
IPv6 header Routing header Fragment header fragment of TCI	P
header + data	
Next Header = Next Header = Next Header =	
Routing Fragment TCP	
· · · · · · · · · · · · · · · · · · ·	

Hop-by-Hop Options (0) Routing (43) Fragment (44) Destination Options (60) Authentication (51) Encapsulating Security Payload (50)

Text Representation of Addresses

(RFC5952)

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX X Hexadecimal Digit, 4 Bits (0-9, a-f) : separates "Hextets" (4 Hex Digits) Notation Rules

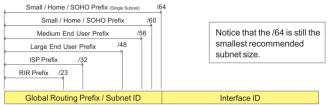
- Eliminate leading zeros in all Hextets
- Longest sequence of 2 or more Hextets of zeros is replaced by :: (used only once)
- Hex characters are represented in lowercase ("a", "b", "c", "d", "e", and "f")

Examples

fe80::1

ff02::1:ff52:b0eb 2001:620:100:10a0:c87e:39ff:fe4b:8645

Address Assignment (RFC6177)



Address Types (RFC4291)

2000::/3	Global unicast
::/128	Unspecified
::1/128	Loopback
ff00::/8	Multicast
fe80::/10	Link-Local unicast
fc00::/7	Unique Local (RFC4193)

Reserved Ranges

::/0	Default Route
::ffff:0:0/96	IPv4-mapped Addresses (RFC4291)
2001::/32	Teredo Tunneling (RFC4380)
2001:db8::/32	Documentation (RFC3849)
2002::/16	6to4 (RFC3056)

Multicast Ranges (RFC4291)

ff01::/16	Interface-Local scope
ff02::/16	Link-Local scope
ff04::/16	Admin-Local scope
ff05::/16	Site-Local scope
ff08::/16	Organisation-Local scope
ff0e::/16	global scope

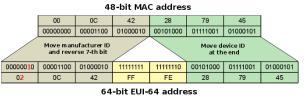
Link-Local Multicast Addresses

ff02::1	All Nodes (RFC4291)
ff02::2	All Routers (RFC4291)
ff02::5	OSPF (RFC5340)
ff02::6	OSPF DR (RFC5340)
ff02::c	SSDP (no RFC)
ff02::16	MLDv2 (RFC3810)
ff02::1:2	All DHCP Agents and Servers
ff02::1:3	LLMNR (RFC4795)
ff02::1:ffxx:xx	xx Solicited-Node Address (RFC4291)

Interface ID

Used to identify Interfaces on a link Always 64 Bits long (RFC4291)

48-Bit Ethernet MAC-Address to EUI-64 Mapping



Privacy Extensions (RFC4941)

Genereate additional random Interface ID (Temporary Address) which is renewed frequently.

Address is used for Internet connections to hide the MAC Address

A Node's required Addresses (RFC4291)

- Link-local address per interface
- All configured unicast addresses
- Loopback address
- All nodes multicast address
- Solicited node multicast address per unicast address
- Multicast address for all member groups

Stateless Address Autoconfiguration -**SLAAC (RFC4862)**

ICMPv6, RS (Router Solicitation), Type133 SA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45) DA: ff02::2 (MAC: 33-33-00-00-00-02)



ICMPv6, RA (Router Advertisement), Type134 SA: fe80::a693:4cff:febc:3582 (MAC: a4-93-4c-bc-35-82) DA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45) Option 3. Prefix Information: 2001:620:100:10a0::/64



- 1. Client creates own link-local unicast address with link-local prefix and EUI-64 Interface ID
- 2. Clients sends ICMPv6 Router-Solicitation to All-Routers link-local multicast Address
- Router replies with ICMPv6 Router-Advertisement, containing the links global routing prefix
- 4. Client create own global unicast address with global routing prefix and EUI-64 Interface ID
- 5. Client performs duplicate address detection against the newly created address

Duplicate Address Detection - DAD (RFC4862)





- 1. Client sends ICMPv6 Neighbor Discovery to his own solicited Node link-local multicast address, expecting no response
- 2. If a host responds, the client need to create another unicast address

Stateless DHCPv6 Service (RFC3736)

- Used to provide DNS Servers to clients
- No client addresses are manged
- Routers must set "o-Flag" in ICMPv6 RA messages





Option 3, Prefix Information: 2001:620:100:10a0::/64 DHCPv6, REQUEST(3); UDP-src: 546; UDP-dst: 547 SA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45) DA: ff02::1:2 (MAC: 33-33-00-01-00-02) (all-dhcp-servers link-local multicast address) Option Request: Domain Search List, DNS recursive Name Server (Vendor specific) DHCPv6, REPLY(7): UDP-src: 547: UDP-dst: 546

SA: fe80::a693:4cff:febc:3582 (MAC: a4-93-4c-bc-35-82) DA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45) DNS Servers (2001:620:100:1000:202, ...), DNS search List (tlab.ch, tlab,int)

- Client sends ICMPv6 RS to all-routers address
- 2. Upon detecting the o-flag, the client sends a DHCPv6 REQUEST to the all-dhcpv6-servers link-local multicast address
- DHCPv6 Server relies with a DHCPv6 REPLY message containing DNS servers and names

Stateful DHCPv6 Service (RFC3315)

- Used to provide DHCP Service to IPv6 nodes
- DHCPv6 Server manages client addresses
- Routers must set "m-Flag" in ICMPv6 RA messages

	ICMPv6, RS, 133
	SA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45)
	DA: ff02::2 (MAC: 33-33-00-00-02)
	ICMPv6, RA, 134, ICMP managed config Flag = 1 (m-Flag)
	SA: fe80::a693:4cff:febc:3582 (MAC: a4-93-4c-bc-35-82)
	DA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45)
	Option 3, Prefix Information: 2001:620:100:10a0::/64
-	
	SOLICIT(1); UDP-src: 546; UDP-dst: 547
	ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45)
DA: ff02::1	:2 (MAC: 33-33-00-01-00-02) (all-dhcp-servers link-local multicast address
DHCPv6,	ADVERTISE(2);
(
	DEOLIEST(2)
DHCPv6.	REQUEST(3)
DHCPv6,	REQUEST(3)

- 1. Client sends ICMPv6 RS to all-routers address
- 2. Upon detecting the m-flag, the client sends a DHCPv6 SOLICIT to the all-dhcpv6-servers link-local multicast address
- 3. DHCPv6 Server relies with a DHCPv6 ADVERTISE message offering a global unicast address
- 4. Client requests the offered address sending a DHCPv6 REQUEST message
- 5. Server acknowledges address assignment with DHCPv6 REPLY message

DNS Server as an RA Option – RDNSS (RFC6106)

Option 25, DNS Servers Option 31, Domain Search List



ICMPv6, RS, 133 SA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45) DA: ff02::2 (MAC: 33-33-00-00-00-02)



- 1. Client sends ICMPv6 RS to all-routers address
- 2. Router replies with ICMPv6 RA message containing global routing prefix and DNS information using an option field

Neighbor Discovery Protocol – NDP (RFC4861)

- Used to map IPv6 addresses and Ethernet MAC addresses
- Replaces Addess Resolution Protocol (ARP) ICMPv6, NS (<u>Neighbor Solicitation</u>), 135 SA: fe80::ca7e:39ff:fe4b:8645 (MAC: c8-7e-39-4b-86-45) DA: ff02::1:ffbc:3582 (MAC: 33-33-FF-bc-35-82)



- 1. Host 1 sends ICMPv6 Neighbor Solicitation to solicited node multicast address
- 2. Host 2 replies with ICMPv6 Neighbor Advertisement containing his Ethernet MAC address