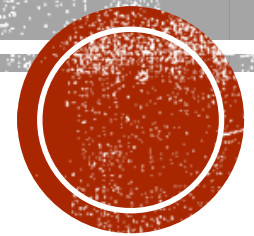
IPv6 Exploits

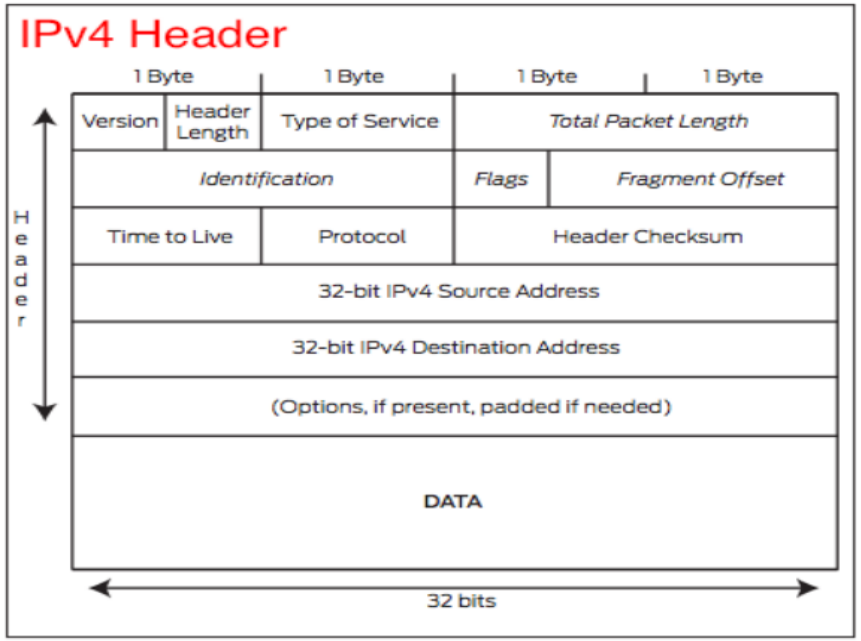
Himanshu Sharma

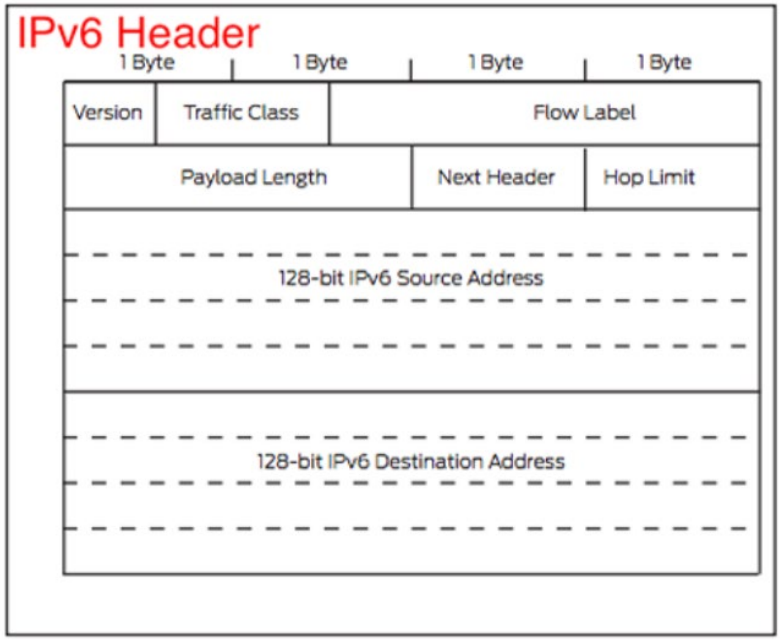
Syed Saad

Siar Ahmad Khan



IPv4 VS IPv6


IPv4 Header
1 Byte
1 Byte
1 Byte
1 Byte
Version
Header Length
Type of Service
Total Packet Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
32-bit IPv4 Source Address
32-bit IPv4 Destination Address
(Options, if present, padded if needed)
DATA
Header
32 bits


IPv6 Header
1 Byte
1 Byte
1 Byte
1 Byte
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
128-bit IPv6 Source Address
128-bit IPv6 Destination Address

Why switch to IPv6?

- Population of Earth

W / Population / World Population

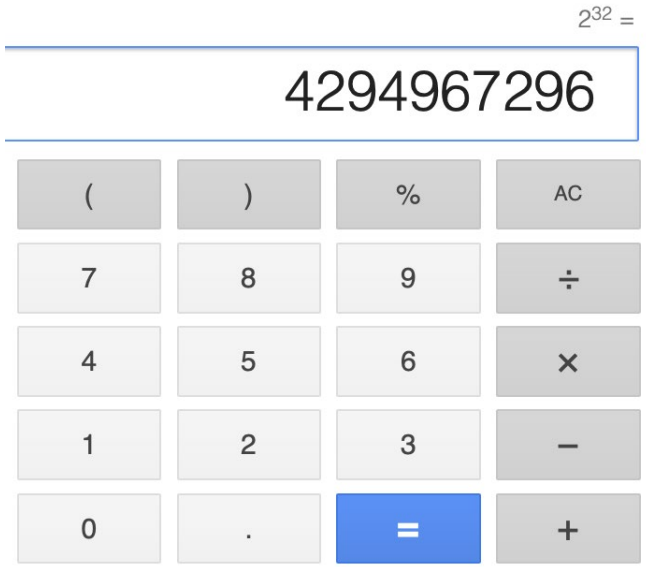
Current World Population

7,676,691,666

view all people on 1 page >

TODAY	THIS YEAR
Births today **305,969**	Births this year **4,547,984**
Deaths today **128,375**	Deaths this year **1,908,189**
Population Growth today **177,594**	Population Growth this year **2,639,795**

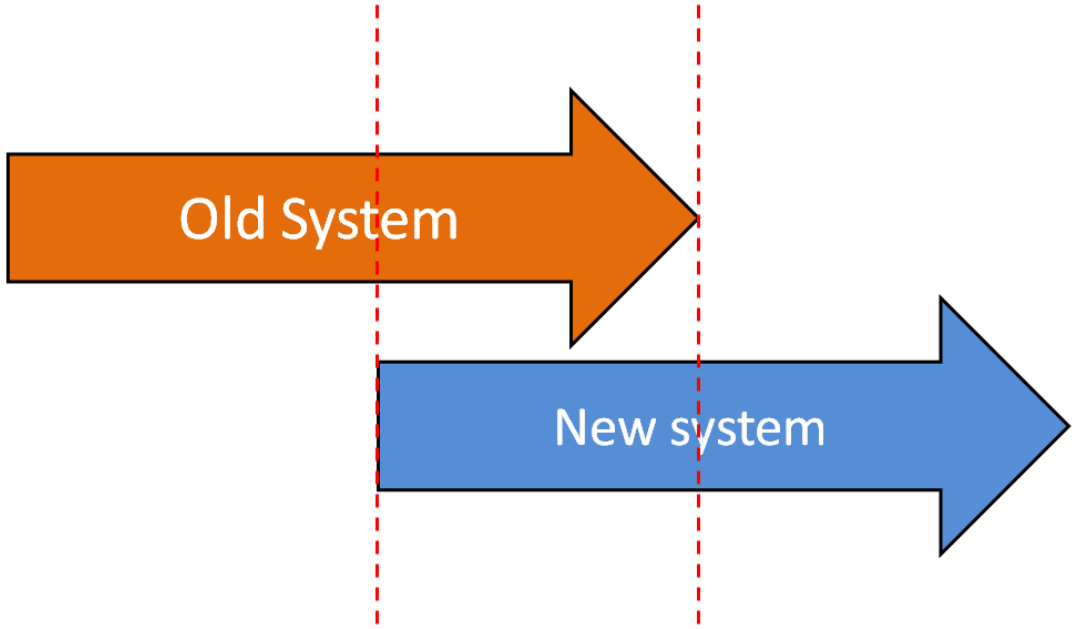
- Number of unique IP's in IPv4



IPV6 SECURITY ISSUES

RELATIVELY NEW PROTOCOL

- IPv6 is not developed enough yet and may encounter unforeseen vulnerabilities in the future.
- Security products such as firewalls are not as available for the IPv6 protocol compared to IPv4.

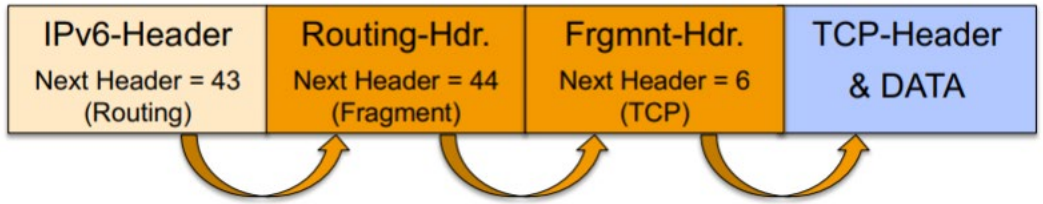


COEXISTING LEADS TO GREATER RISK

- Transition and Dual-stacked Technologies have been deployed which increases complexity in the networks.
- Lack of support from technical personnel

EXTENSION HEADERS

- Extension Headers having varying size.
- Headers are chained.
- Too many EH(s) can harm the network.
- Malicious EH(s) still have to be processed.



FRAGMENTATION ISSUES

Problems

- Can avoid filtering and detection techniques (IDS/IPS evasion techniques).
- Can harm destination devices upon reassembly.

Countermeasures

- Monitor Number of Fragments and discard if over a set amount.
- Block unequal fragments except for last one of a set.

Attacks against the IPv6

1. **Attacks against the IPv6 protocol**
2. **Attacks against ICMPv6**
3. **Attacks against DHCPv6**

Attacks against the IPv6

1. **Attacks against the IPv6 protocol**
2. Attacks against ICMPv6
3. Attacks against DHCPv6

1.1. Multicast:

Via certain multicast messages an attacker can very fast do a reconnaissance attack on a local network.

```
# ping6 ff02::1%br0
PING ff02::1%br0(ff02::1) 56 data bytes
64 bytes from fe80::6e62:6dff:fed1:dfad: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from fe80::5054:ff:fede:b69c: icmp_seq=1 ttl=64 time=0.455 ms (DUP!)
64 bytes from fe80::5054:ff:fe90:de19: icmp_seq=1 ttl=64 time=0.650 ms (DUP!)
64 bytes from fe80::6e62:6dff:fed1:dfad: icmp_seq=2 ttl=64 time=0.046 ms
64 bytes from fe80::5054:ff:fe90:de19: icmp_seq=2 ttl=64 time=0.203 ms (DUP!)
64 bytes from fe80::5054:ff:fede:b69c: icmp_seq=2 ttl=64 time=0.241 ms (DUP!)
64 bytes from fe80::6e62:6dff:fed1:dfad: icmp_seq=3 ttl=64 time=0.064 ms
64 bytes from fe80::5054:ff:fe90:de19: icmp_seq=3 ttl=64 time=0.237 ms (DUP!)
64 bytes from fe80::5054:ff:fede:b69c: icmp_seq=3 ttl=64 time=0.254 ms (DUP!)
^C
--- ff02::1%br0 ping statistics ---
3 packets transmitted, 3 received, +6 duplicates, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.046/0.244/0.650/0.189 ms
```

Source: https://superuser.com/questions/840767/ipv6-multicast-address-for-all-nodes-on-network

Attacks against the IPv6

1. **Attacks against the IPv6 protocol**
2. **Attacks against ICMPv6**
3. **Attacks against DHCPv6**

1.1. Multicast:

Via certain multicast messages an attacker can very fast do a reconnaissance attack on a local network.

1.2. Extension Headers

Inside extension headers an attacker can send information that remain undetected if the intermediary firewalls do not fully check the options of these headers. This kind of attack is called "covert channel".

Attacks against the IPv6

1. Attacks against the IPv6 protocol
2. **Attacks against ICMPv6**
3. Attacks against DHCPv6

2.1. Router Advertisement Spoofing:

If an attacker sends spoofed Router Advertisements inside a subnet, all IPv6 nodes will immediately change their routing tables and store the attacker as one of the default routers

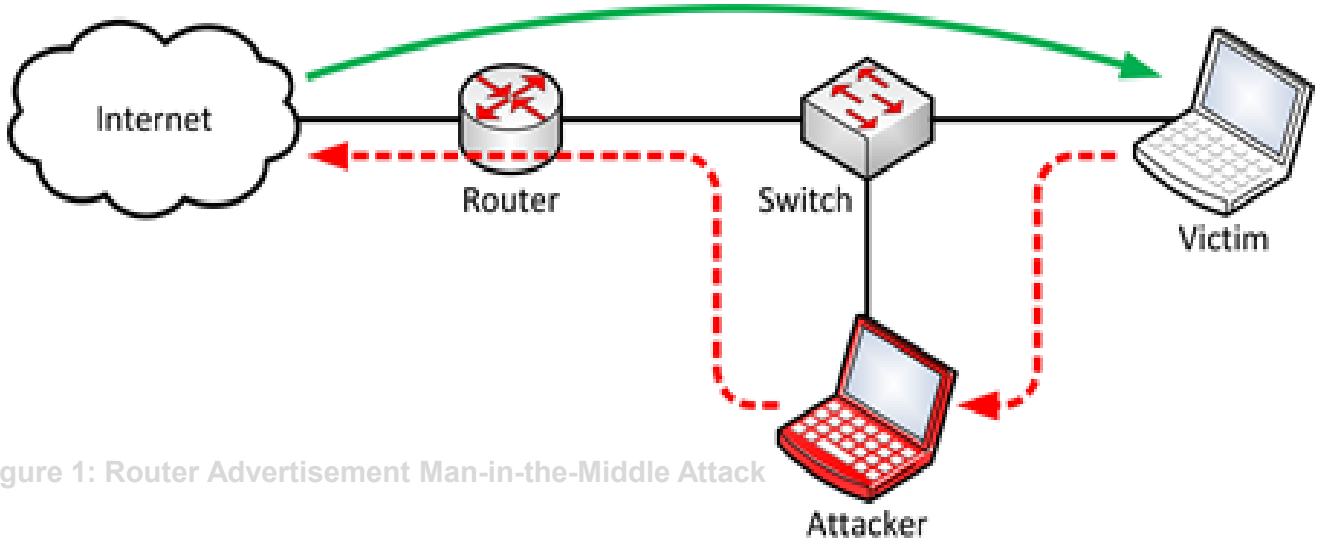


Figure 1: Router Advertisement Man-in-the-Middle Attack

address)

Attacks against the IPv6

1. Attacks against the IPv6 protocol
2. **Attacks against ICMPv6**
3. Attacks against DHCPv6

2.1. Router Advertisement Spoofing:

If an attacker sends spoofed Router Advertisements inside a subnet, all IPv6 nodes will immediately change their routing tables and store the attacker as one of the default routers

2.2. Router Advertisement Flooding

2.3. Neighbor Discovery Spoofing

When the attacker spoofs certain Neighbor Advertisements, he can execute a MITM attack.

2.4. Duplicate Address Detection

A DoS attack is executed if the attacker answers to all Duplicate Address Detection messages (DADs) from a new IPv6 node (with a not yet assigned IPv6 address)

Attacks against the IPv6

1. Attacks against the IPv6 protocol

2. **Attacks against ICMPv6**

3. Attacks against DHCPv6

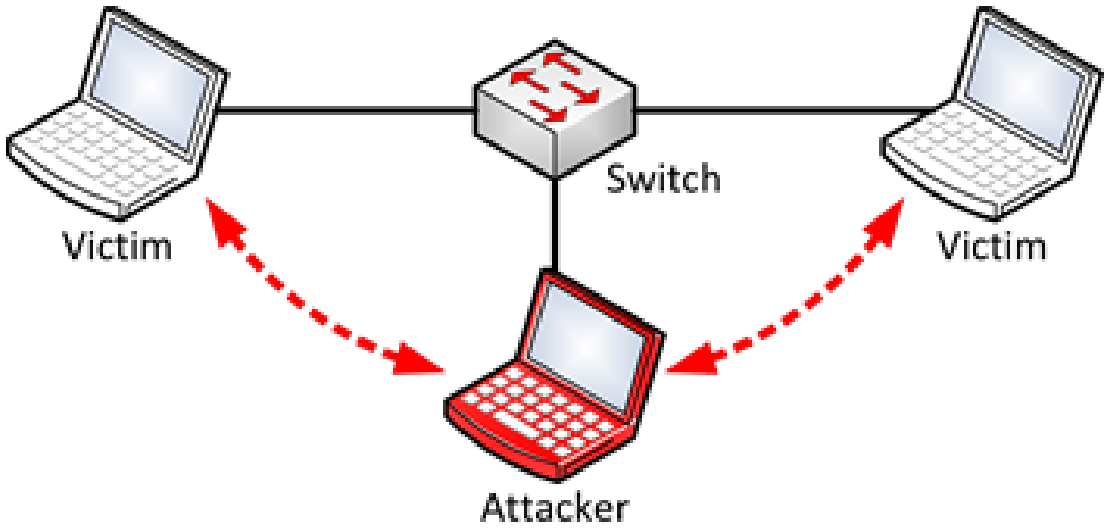


Figure 2: Neighbor Advertisement Man-in-the-Middle Attack

2.1. Router Advertisement Spoofing:

If an attacker sends spoofed Router Advertisements inside a subnet, all IPv6 nodes will immediately change their routing tables and store the attacker as one of the default routers

2.2. Router Advertisement Flooding

2.3. Neighbor Discovery Spoofing

When the attacker spoofs certain Neighbor Advertisements, he can execute a MITM attack.

2.4. Duplicate Address Detection

A DoS attack is executed if the attacker answers to all Duplicate Address Detection messages (DADs) from a new IPv6 node (with a not yet assigned IPv6 address)

Attacks against the IPv6

1. Attacks against the IPv6 protocol
2. **Attacks against ICMPv6**
3. Attacks against DHCPv6

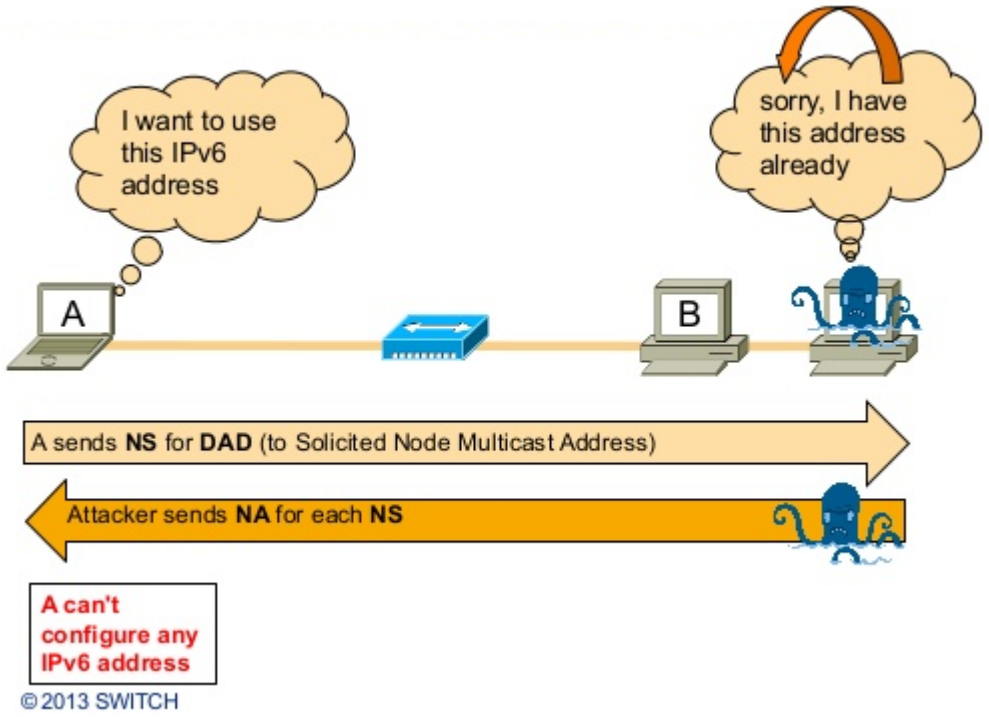


Figure 2: Neighbor Advertisement Man-in-the-Middle Attack

2.1. Router Advertisement Spoofing:

If an attacker sends spoofed Router Advertisements inside a subnet, all IPv6 nodes will immediately change their routing tables and store the attacker as one of the default routers

2.2. Router Advertisement Flooding

2.3. Neighbor Discovery Spoofing

When the attacker spoofs certain Neighbor Advertisements, he can execute a MITM attack.

2.4. Duplicate Address Detection

A DoS attack is executed if the attacker answers to all Duplicate Address Detection messages (DADs) from a new IPv6 node (with a not yet assigned IPv6 address)

Attacks against the IPv6

1. Attacks against the IPv6 protocol
2. Attacks against ICMPv6
3. **Attacks against DHCPv6**

3.1. Address Space Exhaustion

If the concept of stateful DHCPv6 is used, an attacker can exhaust the IPv6 address pool on the server, similar to a DHCPv4 server.

3.2. Rogue DHCPv6 Server

An attacker can also place his own DHCPv6 server inside a network and distribute falsified values, e.g. a spoofed DNSv6 server address.

Figure 3: Rogue DHCPv6 Server

Attacks against the IPv6

1. Attacks against the IPv6 protocol
2. Attacks against ICMPv6
3. **Attacks against DHCPv6**

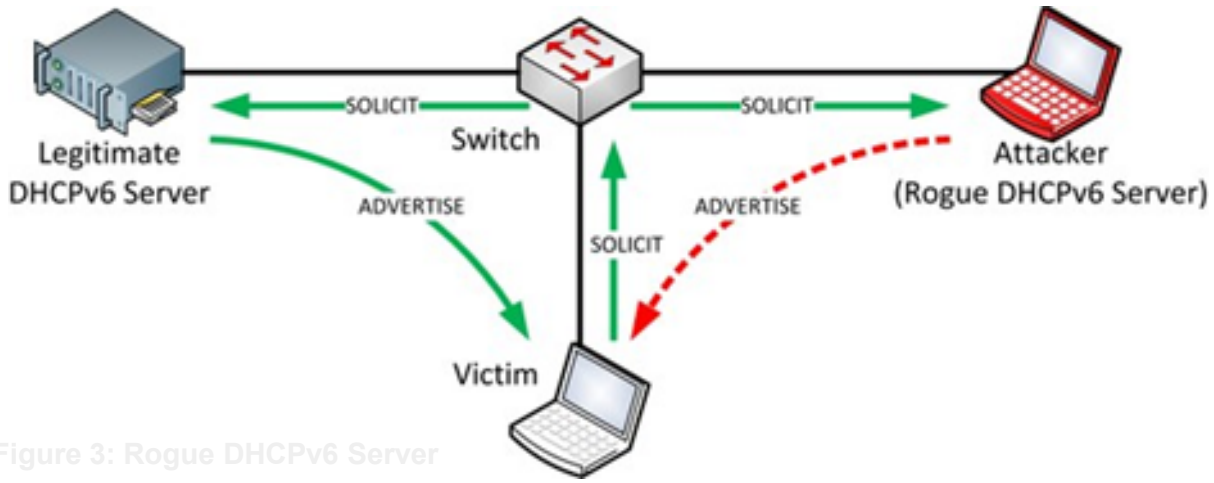


Figure 3: Rogue DHCPv6 Server

3.1. Address Space Exhaustion

If the concept of stateful DHCPv6 is used, an attacker can exhaust the IPv6 address pool on the server, similar to a DHCPv4 server.

3.2. Rogue DHCPv6 Server

An attacker can also place his own DHCPv6 server inside a network and distribute falsified values, e.g. a spoofed DNSv6 server address.

MAC Address from IPv6

- Step 1

Take your MAC address

(52:74:f2:b1:a8:7f)

```
C:\Users\ABC>ipconfig/all
```

- Step 2

Add ff:fe to the middle of MAC address

So, we have 52:74:f2:**ff:fe**:b1:a8:7f

- Step 3

Convert 1st octet from Hexadecimal to Binary

52 equals 0101 0010

- Step 4

Invert index number 6

0101 0010 becomes 0101 0000

- Step 5

Converting Binary to Hexadecimal

0101 0000 equals 50

hexadecimal	binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

- Step 6

New version after conversion

50:74:f2:ff:fe:b1:a8:7f

- Step 7

Add the local prefix (fe80)

fe80:: 50:74:f2:ff:fe:b1:a8:7f

- Step 8

Celebrate. You did it!

Conclusion

- IPv6 is slightly better than IPv4 in terms of security but IPv6 is not necessarily more secure than IPv4
- From a top view, the vulnerability concepts have not changed that much
- Take some time until all network and security devices have a full adoption of all IPv6 defense methods
- Some attacks are possible against the transition methods from IPv4 to IPv6
- IPv6 stack implementations in all operating systems will have errors. That means: Not only the generic IPv6 security issues but also application specific vulnerabilities that are new due to the usage of IPv6.

References

- https://www.whatismyip.com/ip-address-lookup/
- https://whatismyipaddress.com/ip-addresss
- https://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html
- https://www.juniper.net/us/en/products-services/what-is/ipv4-vs-ipv6/
- https://dl.packetstormsecurity.net/papers/general/security-IPv6.pdf
- https://www.first.org/resources/papers/conf2018/Herberg-Frank_FIRST_20180624.pdf