IPv6

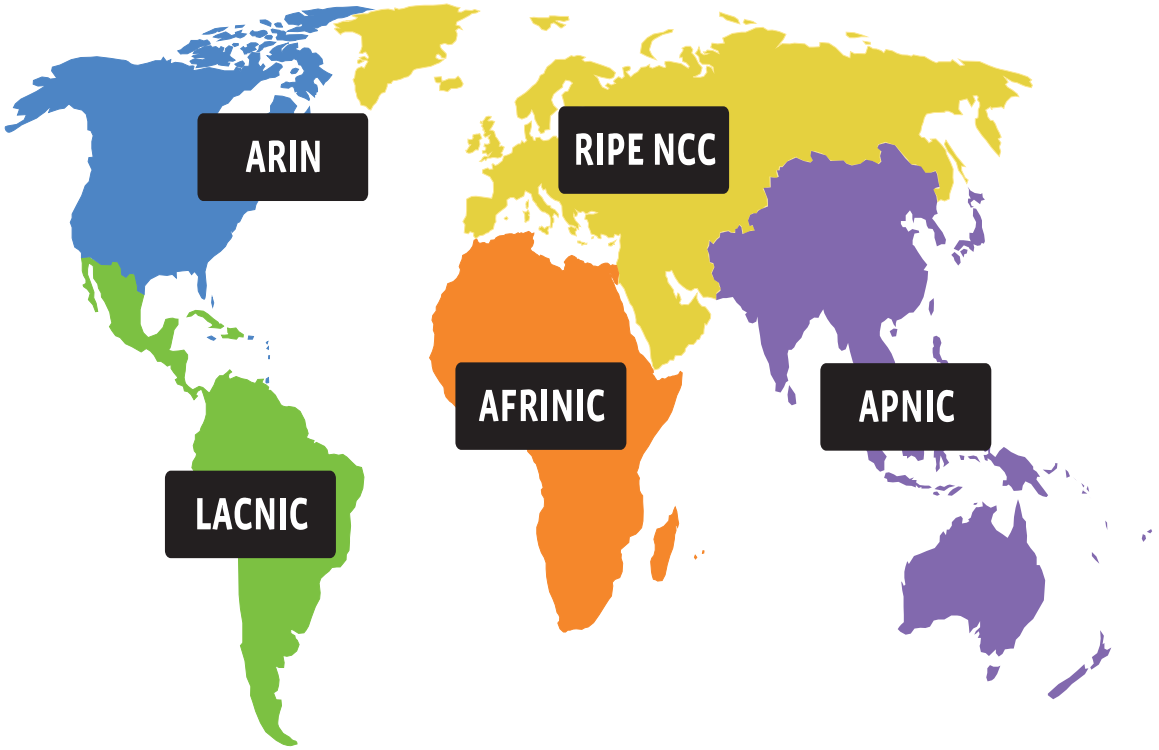
Introduction & Security Issues

Vincent Ryan

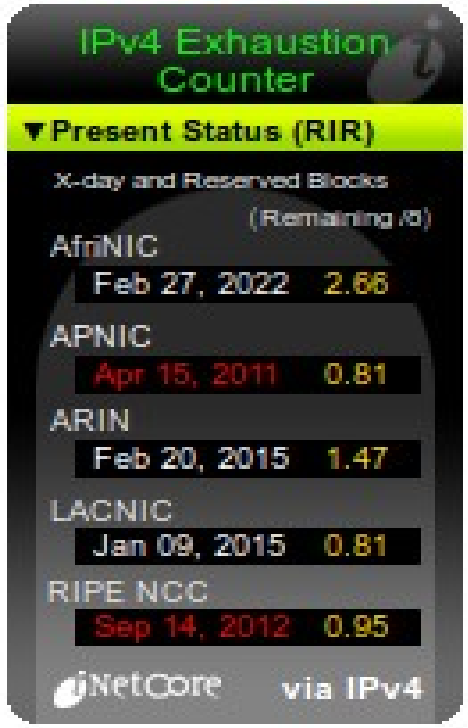
Background

- developed by the Internet Engineering Task Force (IETF) and ratified in 1998.
- 128-bit address range.

IPv4 Exhaustion



source:http://www.iana.org/numbers



source:inetcore.com

Background

- Enough IP addresses for the next decades:
- 2^{128}=340,282,366,920,938,463,463,374,607,431,768,211,456
- $= 3.4 * 10^{38}$,
- $= 6.67 * 10^{17}$ addresses per mm^2 surface of the earth. (But due to the division of network- and interface-IDs, this quantity is not realisable.)

HighLights

- Longer IP address
- ICMP, IGMP and ARP all rolled into ICMPv6
- No broadcast addresses

Some IPv6 Enabled Sites

ipv6.google.com

www.v6.facebook.com

ipv6.cnn.com

ipv6.netflix.com

source : www.sixxs.net/wiki/IPv6_Enabled_Websites

The Address

IPv6 address

fe80:0000:0000:0000:0200:f8ff:fe21:67cf

fe80:0:0:0:200:f8ff:fe21:67cf

fe80::200:f8ff:fe21:67cf

IPv6 address

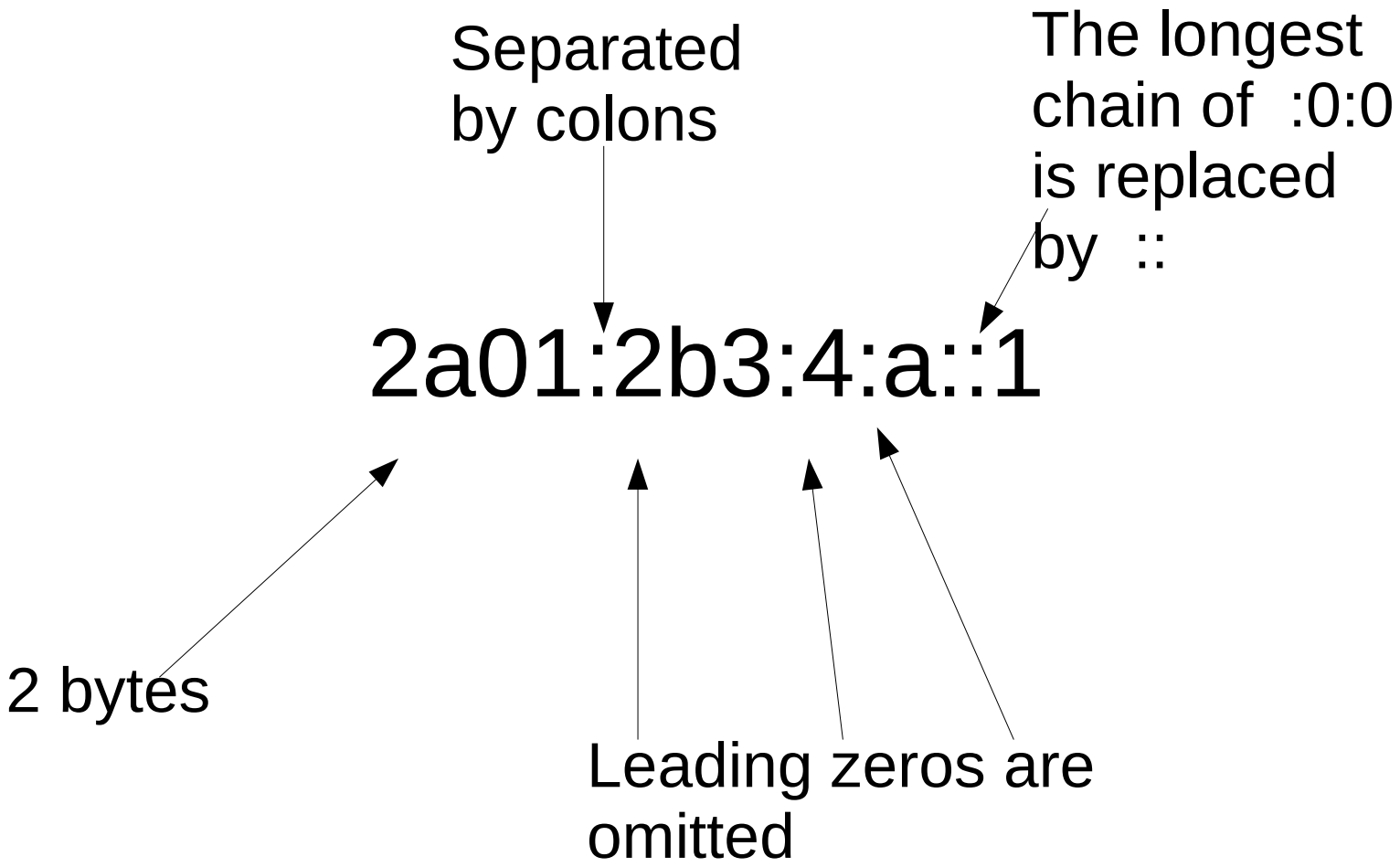
Last 2 fields may be represented in IPv4 “dotted decimal” form

e.g. 0:0:0:0:0:ffff:192.168.0.1 or ::ffff:192.168.0.1

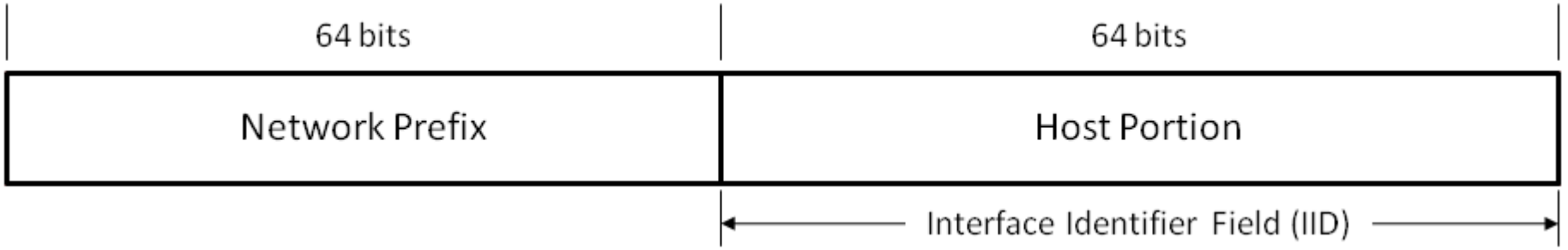
“[]” are used around the address for representation in URLs

http://[3ffe:a:b:c::1]:port/dir

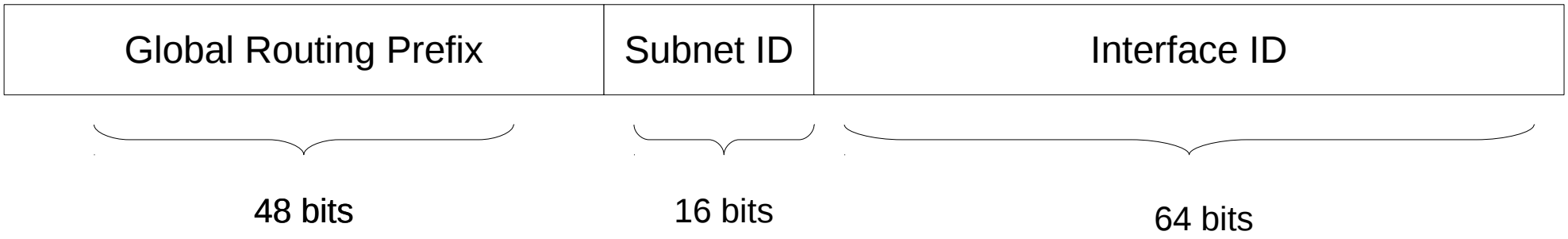
The loopback address, i.e. the moral equivalent to IPv4’s 127.0.0.1 , is ::1


Separated
by colons
The longest
chain of :0:0
is replaced
by ::
2a01:2b3:4:a::1
2 bytes
Leading zeros are
omitted

Ip6 address


64 bits
64 bits
Network Prefix
Host Portion
Interface Identifier Field (IID)

IPv6 address



Router Solicitation & Advertisement

- The Router Solicitation message is sent by a node in order to discover any routers on the link. It is sent to the all-routers multicast address ff02::2.
- If a router is present on the link, it answers immediately with a Router Advertisement.
- Additionally, the router sends out Router Advertisements at a regular interval.

IPv6 Myths

Everything in IPv6 is encrypted??

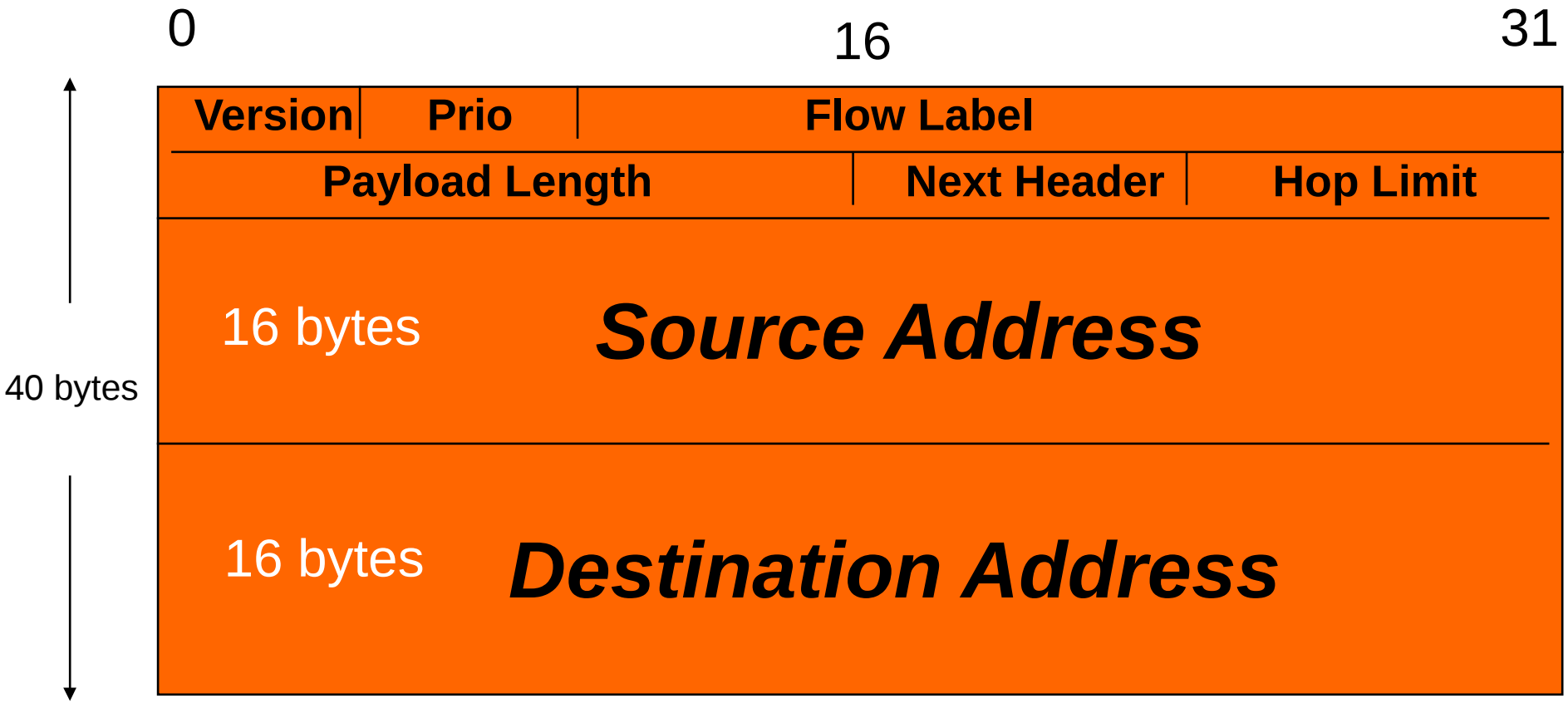
- IPSec is a MANDATORY component of the IPv6 stack, and by being more universally available, it may make it easier to configure
  - But you may still have to install additional software.

My Network will be more exposed??

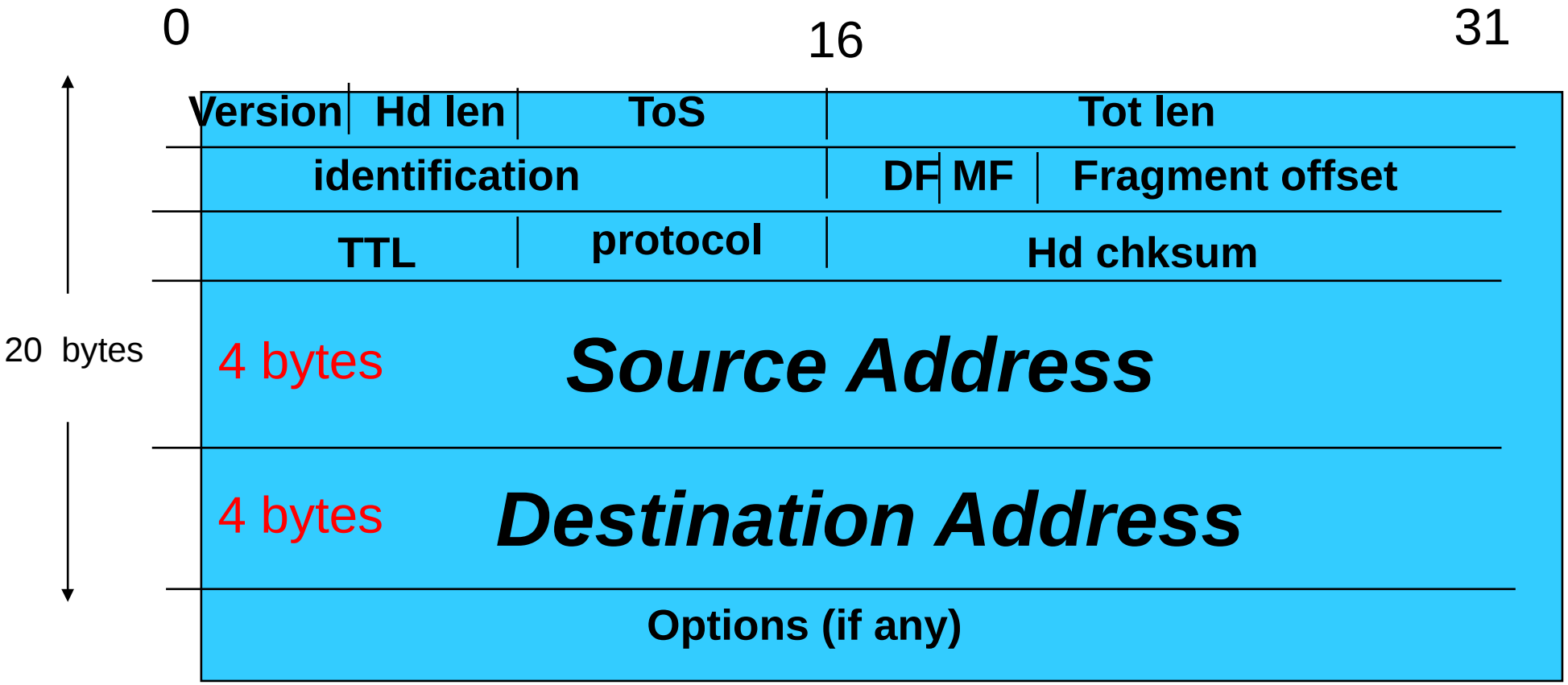
- NAT never was supposed to be a security feature, and it doesn’t help against most client attacks eg email attachments.

The Header

IPv6 Header (40 bytes)



IPv4 Header (20 bytes)



Daisy Chain of Headers

ICMPv6

ICMPv6

- ICMPv6 is mandatory for IPv6 operation

- ICMPv6 types are defined with firewalls in mind:
  - Messages with a code of 1-127 are considered error messages, and 128 and up are informational messages.

Some Security Issues

Blacklisting

- With the introduction of ipv6, a huge quantity of new internet addresses is available, and those addresses could be used as sources for DDoS attacks.
- It will be more difficult to identify and **blacklist** the addresses involved, now that the attacker has an availability that is significantly increased.

Not as well understood

- Security products such as firewalls and Network Intrusion Detection Systems have less support for the IPv6 protocols than for their IPv4 counterparts.

- Technical personnel have less confidence with the IPv6 protocols than with their IPv4 counterparts. This creates an increased likelihood that security implications are overlooked when the protocols are deployed.”

Log Analysis using grep won't work

- log analysis tools at first sight might seem to work fine with IPv6,
- but they often don't "normalize" the addresses, meaning that
  - 2001:db8::1 is not considered equal to
  - 2001:0db8::1 or
  - 2001:0db8:0000:0000:0000:0000:0000:0001

How is the IP address assigned?

Recall: The first 64 bits specify the network, while the second half of the address identify the host.

1. Derived from MAC addr (SLAAC)
2. Privacy Enhanced Temporary Addresses
3. DHCPv6

SLAAC

1. After booting, each interface generates its link-local unicast address with a prefix of fe80::

and an interface ID which got using EUI-64

2. The interface performs a **Duplicate Address Detection** (DAD) for its tentative link-local unicast address by sending a Neighbor Solicitation message.

Privacy Enhanced Temporary Addresses

An address is picked randomly, and, once a day, the host will pick a new random interface ID.

The host will check if the new address is already in use, again using DAD.

But, how do we show who owned the address?

DHCPv6

DHCPv6 can be used just like DHCP in IPv4

For accountability, make sure that these are the only addresses used.

For example, you could use a firewall to restrict network access to allow only access from addresses within the valid DHCP range.

Security Issue: Firewalling

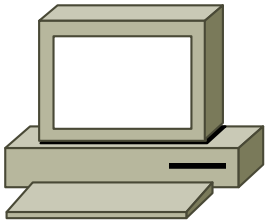
- Note that if you open an IPv4 port on the Windows firewall, allowing it in, you are also opening the IPv6 port.
- In the linux firewall, we have iptables for IPv4 and **ip6tables** for IPv6, so opening a port on say IPv4 will not open the port on IPv6
- Note that opening a service (eg SSH), usually opens the port (22) for both IPv4 and IPv6
- DEMO

- Extension headers can pose a challenge to firewalls.
- IPv4: max IPv4 header size is 60 bytes
- IPv6: one or more extension headers may be inserted between IPv6 and transport header (TCP,UDP,ICMP).
- Some of these extension headers can be up to 2kBytes in length!!

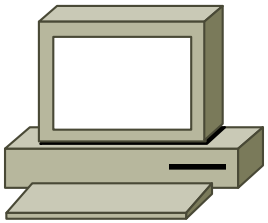
- THC IPv6 test suit includes a tool "firewall6" that can be used to create various odd and malformed IPv6 packet to test firewalls.
- Several of the options produce packets with headers exceeding 2,000 bytes.
- These tests crashed Kaspersky's personal firewall (March 2013)
  - A packet with a large "Destination Header" caused the firewall to crash and drop all traffic.

Other Security Issues

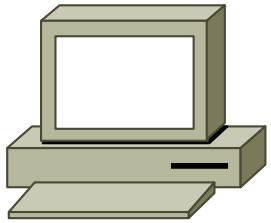
ARP Cache Poisoning



Victim 1



MITM



Victim 2

ARP Cache Poisoning

No ARP, so does this rule out ARP cache poisoning?

Tools: parasite6, NDPMon

DAD Denial of Service Attack

- A host sends a Neighbour Solicitation for an IP address that it wants to use for itself. If there is no answer, the address is free and the host can use it.
- However, the tool dos-new-ipv6 will always respond to every NS request saying that the IP address is in use. So the host can never join the network

RA based attack

- Gets rid of the default router on a LAN as follows:
- The attacker sends his/her own RA, but spoofs the Router Address of the default Router, and add a parameter that says that the its lifetime is 0.
- The hosts will think that the router is announcing that it is no longer available
- (The hosts see no router now, so according to the RFC, they are to assume that everything is local. - the entire global IPv6 network is local)
- The attacker then sends his/her own RA, and becomes the default router for the LAN.

Another RA based attack

- RA Flooding:
- Send out a huge number of RAs coming from seemingly different routers in a LAN
- Many routers and firewalls CPUs run at 100%
- Command: flood_router6 eth0 (don't do this!)

Attack Tools

Some IPv6 Attack Tools

- Scapy: Allows crafting IPv6 packets at will
- THC IPv6 Attack Suite: basic library to create IPv6 packets plus good number of tools

Using nmap on ip6

- Scan your local subnet for all IPv6-enabled systems in one shot:

```
# nmap -6 –script=targets-ipv6-multicast-*
```

- Port scan the top 10000 ports on these assets:

```
# nmap -6 --script=targets-ipv6-multicast-*
--script-args=newtargets -PS --top-ports=10000
```

TOPERA

- Topera allows for more stealthy port scans using IPv6.
- Adds a number of destination header options to the scan.
- Many IDS systems ignore the ext headers!!
- http://www.iniqua.com/labs/topera-invisible-tcp-scanner/?lang=en

Privacy

- Internet of Things
- Autoconfiguration

That's all

vincent.ryan@cit.ie

@vincentrya