M2 CyberSecurity
Security Architecture: network, system, key management, cybersecurity of industrial system.

Systems and Network Security

Florent Autréau - florent.autreau@imag.fr
2016 /2017

Network Security - Part 4

- Introduction
- Threat landscape
- Cryptography and Network Security
- Network Security – Vulnerabilities/Protection
  - IPv6 Overview
  - IPv6 Security considerations

IPv6

- IPv4 allows over 4 billion computers (but not really) – inefficient subnetting is using these up.
- IPv6 allows 16 octet addresses (4 octets in IPv4).
- $3x10^{38}$ addresses (> Avogadro's number). $7x10^{23}$ IP addresses per square meter of the earth's surface.
- Why so many? Electrical devices may want IP addresses – your house could be its own subnetwork. Why NOT?
- Better security than current IP(v4).
- Allow "roaming hosts".
- Pay more attention to type of service (for real time data).

IPv6 Features

- Larger Address Space
- Aggregation-based address hierarchy

Efficient backbone routing

- Efficient and Extensible IP datagram
- Stateless Address Autoconfiguration
- Security (IPsec mandatory)
- Mobility

Brief comparision of IPv6 and IPv4

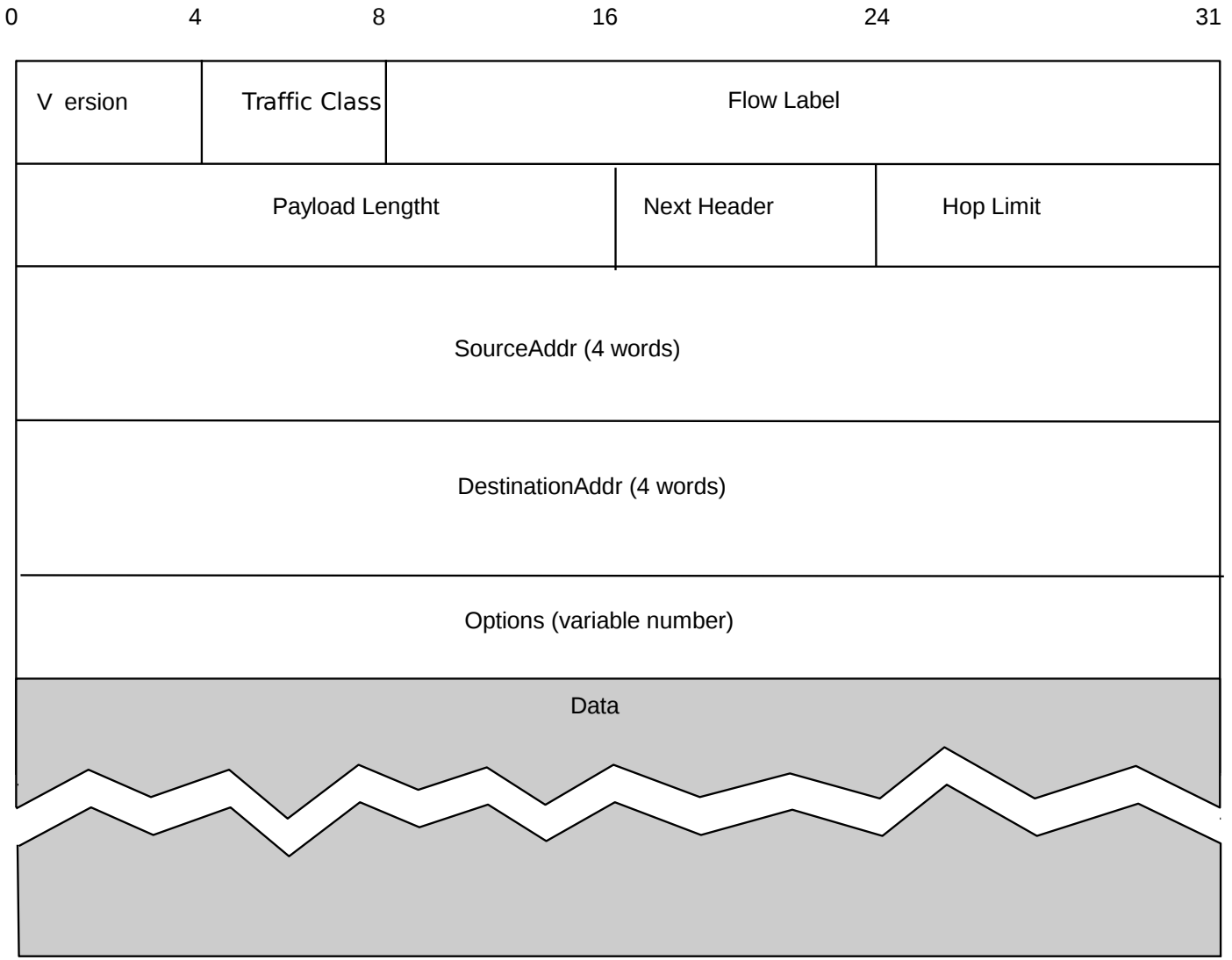
- IPv6 and IPv4 are very similar in terms of functionality (but not in terms of mechanisms)

	IPv4	IPv6
Addressing	**32 bits**	**128 bits**
Address resolution	**ARP**	**ICMPv6 NS/NA (+ MLD)**
Auto-configuration	**DHCP & ICMP RS/RA**	**ICMPv6 RS/RA & DHCPv6 (optional) (+ MLD)**
Fault Isolation	**ICMPv4**	**ICMPv6**
IPsec support	**Optional**	**Mandatory (to "optional")**
Fragmentation	**Both in hosts and routers**	**Only in hosts**

Address Space & Notation

- Allocation is classless
  - Prefixes specify different uses (unicast, multicast, anycast)
    - Anycast: send packets to nearest member of a group
  - Prefixes can be used to map v4 to v6 space and visa-versa
  - Lots of flexibility with 128 bits!
- Standard representation is set of eight 16-bit values separated by colons
  - 47CD:1234:3200:0000:0000:4325:B792:0428
  - If there are large number of zeros, they can be omitted with series of colons
    - Eg. 47CD:1234:3200::4325:B792:0428
  - Address prefixes (slash notation) are the same as v4
    - Eg. FEDC:BA98:7600::/40 describes a 40 bit prefix

Ipv6 Packet


0
4
8
16
24
31
V ersion
Traffic Class
Flow Label
Payload Lengtht
Next Header
Hop Limit
SourceAddr (4 words)
DestinationAddr (4 words)
Options (variable number)
Data

Packet Format

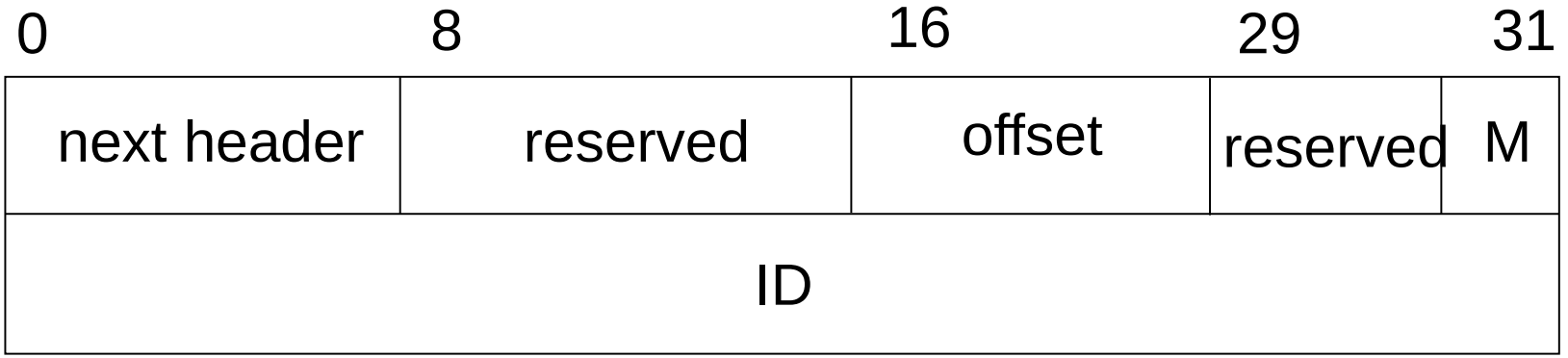
- Simpler format than v4
- Version = 6
- Traffic class same as v4 ToS
- Treat all packets with the same Flow Label equally
  - Support QoS and fair bandwidth allocation
- Payload length does not include header –limits packets to 64KB
  - There is a “jumbogram option”
- Hop limit = TTL field
- Next header combines options and protocol
  - If there are no options then NextHeader is the protocol field
- Options are “extension header” that follow IP header
  - *Ordered* list of tuples – 6 common types
  - Eg. routing, fragmentation, authentication encryption…

Key differences in header

- No checksum
  - Bit level errors are checked for all over the place
- No length variability in header
  - Fixed format speeds processing
- No more fragmentation and reassembly in header
  - Incorrectly sized packets are dropped and message is sent to sender to reduce packet size
  - Hosts should do path MTU discovery
  - But of course we have to be able to segment packets!
    - What about UDP packets?

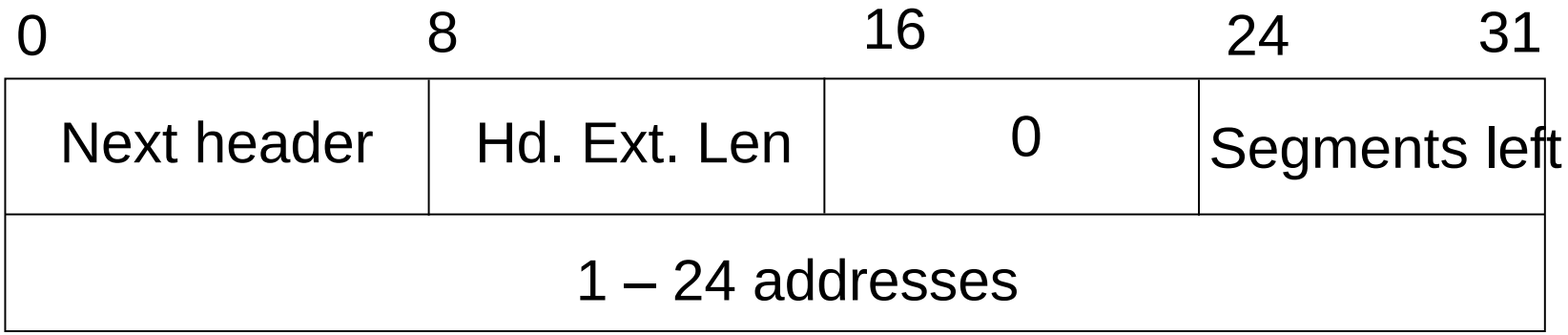
Fragmentation Extension

- Similar to v4 fragmentation
  - Implemented as an extension header
    - Placed between v6 header and data (if it is the only extension used)
  - 13 bit offset
  - Last-fragment mark (M)
  - Larger fragment ID field than v4
- Fragmentation is done on end host



Routing Extension

- Without this header, routing is essentially the same as v4
- With this header essentially same as the source routing option in v4
  - Loose or strict
- Header length is in 64-bit words
- Up to 24 addresses can be included
  - Packet will go to nearest of these in “anycast” configuration
- Segments left tracks current target



Transition from v4 to v6

- *Flag day* is not feasible
- Dual stack operation – v6 nodes run in both v4 and v6 modes and use version field to decide which stack to use
  - Nodes can be assigned a *v4 compatible v6 address*
    - Allows a host which supports v6 to talk v6 even if local routers only speak v4
    - Signals the need for tunneling
    - Add 96 0’s (zero-extending) to a 32-bit v4 address – eg. ::10.0.0.1
  - Nodes can be assigned a *v4 mapped v6 address*
    - Allows a host which supports both v6 and v4 to communicate with a v4 hosts
    - Add 2 bytes of 1’s to v4 address then zero-extend the rest – eg. ::ffff:10.0.0.1
- Tunneling is used to deal with networks where v4 router(s) sit between two v6 routers
  - Simply encapsulate v6 packets and all of their information in v4 packets until you hit the next v6 router

IPv6 Issues

- Address length: usable addresses vs. overhead
- Hop limit: is 65K necessary?
- Max. Pkt. Size: Larger BW calls for larger packets.
- Is the checksum necessary?
- How do servers handle both types of packets?
- Is security necessary in IP?
  - How is it best implemented?
- DNS can be very important in the transition – how?

More Issues foreseen ...

- There is much less experience with IPv6 than with IPv4
- IPv6 implementations are less mature than their IPv4 counterparts
- Security products (firewalls, NIDS, etc.) have less support for IPv6 than for IPv4
- The complexity of the resulting network will increase during the transition/co-existance period:
  - Two internetworking protocols (IPv4 and IPv6)
  - Increased use of NATs
  - Increased use of tunnels
  - Use of other transition/co-existance technologies
- Lack of well-trained human resources

...and even then, in many cases IPv6 will be the only option to remain in this business

New Security Issues in IPv6

- Many of the new protocol’s characteristics can be utilized to accomplish attacks to systems and networks
- IPv6 deployment calls for deep understanding of the protocol, its requirements and security issues. Careful planning is necessary to lessen the possibility of malicious exploitation

IPv6 Security Characteristics

- Based upon IPv4 experiences the new protocol incorporates a number of elements that address known security problems.
- Support for some IPsec features:
  - Authentication headers
  - Encryption headers
  - These can be used to implement specific security policies. Separate implementation allows for a degree of flexibility when implementing a particular policy.

Network Reconnaissance

- Big number of possible IPs complicates the task of discovery of operating systems and services using host and port scanning
  - Default network size is 2^{64} IPs – very difficult to cover it by packet probes
- Weaknesses:
  - Usually main systems get assigned “easy to remember” addresses
  - DNS servers keep system data
  - IPv6 neighbor-discovery data
  - Special multicast addresses for various types of network recourses (routers, DHCP servers etc.)

Access Control

- One Interface may simultaneously have various addresses
  - Link local , site local, global unicast
  - The administrator may enable global unicast addresses only for devices that must access the internet.
- Extension Headers in IPv6 may be used to bypass the security policy
  - E.g. routing headers have to be accepted at specific devices (IPv6 endpoints)
- In IPv6 some ICMP and (link-local) Multicast messages are required for the correct operation of the protocol
  - The firewalls should be appropriately configured only to allow the right messages of these types
  - The IPv4 ICMP security policy must be appropriately adapted for ICMPv6 messages

Packet Spoofing

- Possible for levels 3 and (particularly) 4
- The address allocation method offers a new characteristic for the control of packets with spoofed source address
  - Globally aggregated nature of address allocation means that addresses are assigned from bigger to smaller groups. At different stages of the routing procedure filters can be set up to check and block wrong source addresses.
  - The big number of available IPv6 addresses allows an attacker to use spoofed, yet from valid sources, addresses

ARP and DHCP attacks

- Devices are mislead to take wrong IPs, or be configured with malicious settings
- IPv6 does not provide any extra security on this issue
  - The stateless autoconfiguration procedure (based on ICMPv6) automatically assigns addresses. However, DHCP servers could possibly be used in the future to provide extra service information
  - DHCPv6 is not considered “mature”, yet
  - The same process (stateless autoconfiguration) can be hijacked
  - ICMPv6 neighbor discovery replaces ARP, but suffers from the same problems

Amplification (DDoS) Attacks

- There are no broadcast addresses in IPv6
  - This would stop any type of amplification/"Smurf" attacks that send ICMP packets to the broadcast address
  - Global multicast addresses fro special groups of devices, e.g. link-local addresses, site-local addresses, all site-local routers, etc.
- IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses.
  - Many popular operating systems follow the specification
  - Still uncertain on the danger of ICMP packets with global multicast source addresses

Mixed environments v4/v6

- There are security issues with the transition mechanisms
  - Tunnels are extensively used to interconnect networks over areas supporting the “wrong” version of protocol
  - Tunnel traffic many times has not been anticipated by the security policies. It may pass through firewall systems due to their inability check two protocols in the same time
  - Such checks also set high demands for processing power and computing recourses
  - The problem is deteriorated by the fact that many tunneling mechanisms are operating automatically

Mixed environments v4/v6 – 6to4

- 6to4 provides the main mechanism for communications of IPv6 systems or networks over IPv4
  - Automatic and dynamic connectivity between dual stack IPv6 systems within IPv4 networks (6to4 hosts) and native IPv6 areas
  - 6to4 gateways acquire an IPv6 address with the prefix 2002: based on their IPv4 address

Mixed environments v4/v6 – 6to4 (2)

- One IPv6 network may send attack traffic to an IPv4 system by constructing packet with the appropriate IPv6/6to4 destination address. Corresponding tunnels are implemented dynamically.
- The same type of attack may be initiated from an IPv4 system concealing the source. The path is:

  System IPv4 - 6to4 router and removal of the IPv4 address – Target IPv4 system (its address described in IPv6/6to4)

  - DDoS attack potentiality rather low due to ressource limitations at the 6to4 router
  - It’s possible to use different 6to4 nodes for each direction
  - The mechanism may also be used for Reflection attacks

Viruses, Worms and automated attack tools

- The effect of the new protocol to the worms abilities to propagate is not know
- DDoS attack tools operating in IPv6 environment are already available, e.g. 6To4DDos.
- Some attack programs incorporate code that allows them to operate in IPv6 too
  - Such a worm has already been detected by the Honeynet project

Common IPv4 - IPv6 attacks

- Packet sniffing
- Application Layer Attacks
- Rogue devices
- “Man-in-the-middle” attacks
- DDoS traffic attacks

Security recommendations

- Automatic configuration security mechanisms that mask the MAC address may also be used to conceal and attacker.
- Assign global addresses only to systmes that require Internet connectivity
- Non-trivial addresses for critical systems
- Filter non necessary services at the firewall
- Selective ICMPv6 filtering
- Keep the systems and application security level current by deploying patches
- Careful selection of the cases when Extension Headers should be allowed

Security recommendations (2)

- The firewall should have the ability to check fragmented packets
- Filter packets with wrong source addresses
- Traceback procedures at levels 2 and 3 should be available to show concealed attackers
  - The big number of available addresses may be used to hide the attackers.
- Disallow packets with multicast source addresses
- It’s better to avoid “translation” mechanisms between IPv4 and IPv6 and use dual stack instead

Security recommendations (3)

- Preferably, static tunnel configuration
- Only authorized systems should be allowed as tunnel end-points

Conclusion

- Beware of IPv6 marketing and mythology!
- While IPv6 provides similar features than IPv4, it uses different mechanisms. – and the devil is in the small details
- The security implications of IPv6 should be considered before it is deployed (not after!)
- Most systems have IPv6 support enabled by default, and this has implications on “IPv4-only” networks!
- Even if you are not planning to deploy IPv6 in the short term, most likely you will eventually do it
- It is time to learn about and experiment with IPv6!