An Overview of IPv6 Security

UKNOF42 January 2019

Dr David Holder CEng FIET MIEEE

david.holder@erion.co.uk

Erion

Overview of IPv6 Security

- Common Misconceptions about IPv6 Security
- IPv6 Threats and Vulnerabilities
- IPv6 Security Features
- The Future for IPv6 Security

Erion

Overview of IPv6 Security

- **Common Misconceptions about IPv6 Security**
- IPv6 Threats and Vulnerabilities
- IPv6 Security Features
- The Future for IPv6 Security

Erion

The Top Two Misconceptions

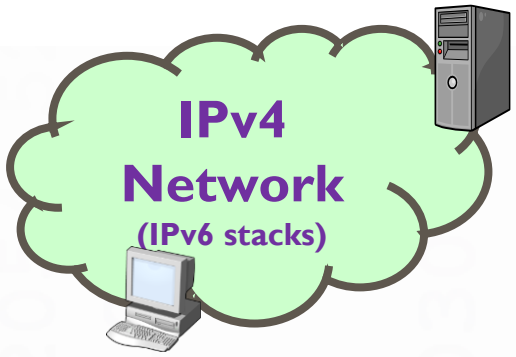
1. IPv6 is *more* secure than IPv4 ✗
2. IPv6 is *less* secure than IPv4 ✗

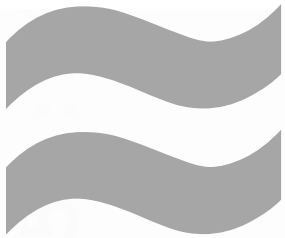
- Both are **WRONG**
- Assume that comparing IPv4 with IPv6 is meaningful
  - it isn't

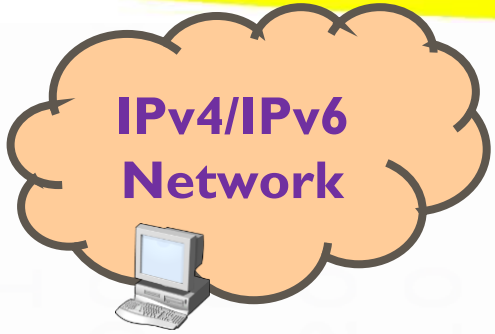
More about why people think this later, but first the truth…

Erion

Reality: IPv6 Dual Stacks





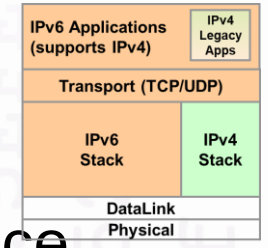


Dual stack devices and operating systems

similar vulnerabilities

Dual stack devices and operating systems

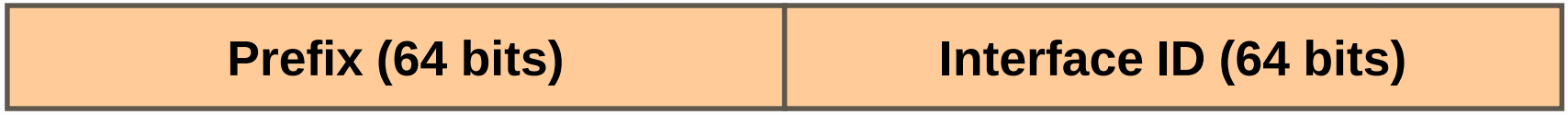
- Today operating systems and devices are **all** dual stack
- IPv6 **on** by default
- IPv4 networks are built on IPv6 dual stacks
- You have a combined IPv4/IPv6 vulnerability surface
- **All** networks should be secured for IPv6 vulnerabilities



Erion

The Third Big Misconception

3. IPv6 is IPv4 with long addresses ✗



- **It isn't;** many complex & subtle differences from IPv4
- ***Even*** addresses are very different:
  - NEW New attributes: length, scope and lifetimes
  - NEW Normal for IPv6 interfaces to have multiple addresses
  - NEW IPv6 addresses can change over time
- DIFFERENT Multicast is very important in IPv6
  - NEW Large number of methods for assigning interface identifiers
- DIFFERENT How addresses are used and managed is different
- DIFFERENT Global addresses are normal

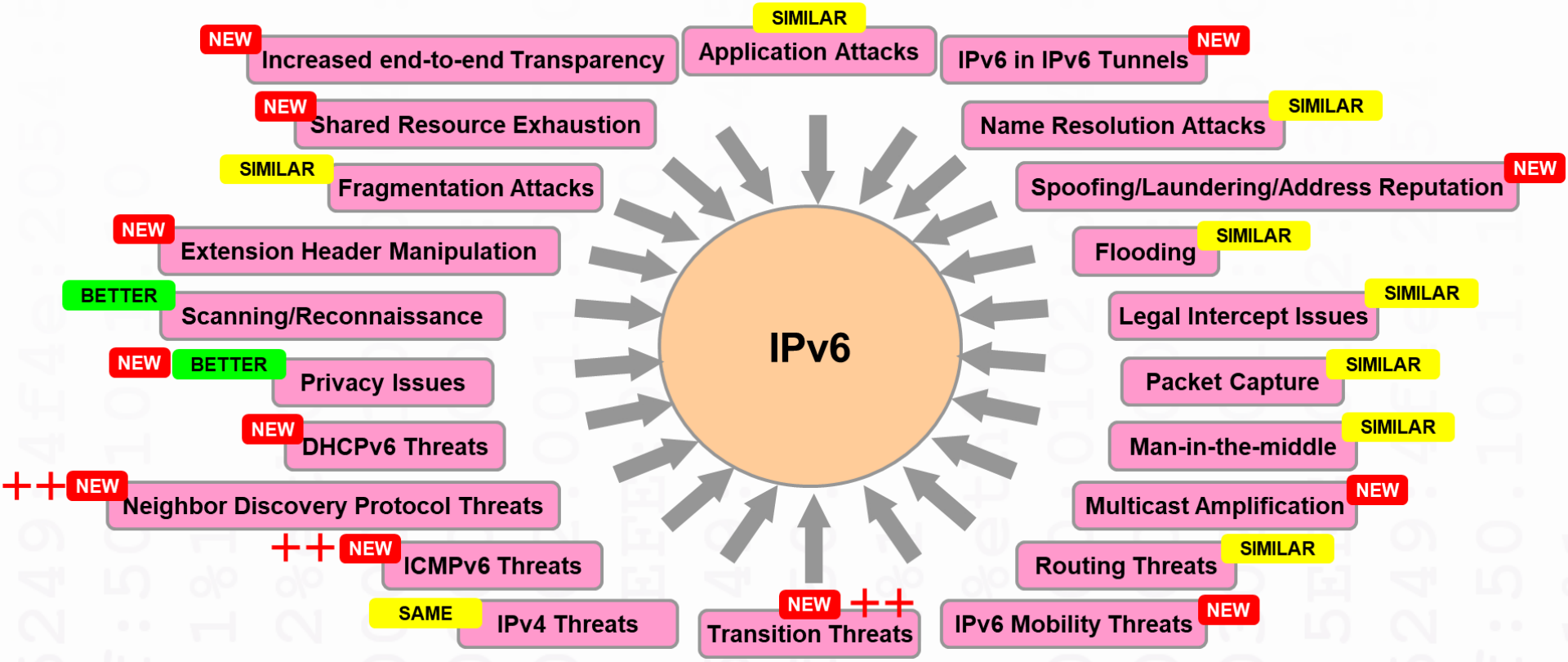
Erion

Overview of IPv6 Security

- Common Misconceptions about IPv6 Security
- **IPv6 Threats and Vulnerabilities**
- IPv6 Security Features
- The Future for IPv6 Security

Erion

IPv6 Vulnerability Surface



Erion

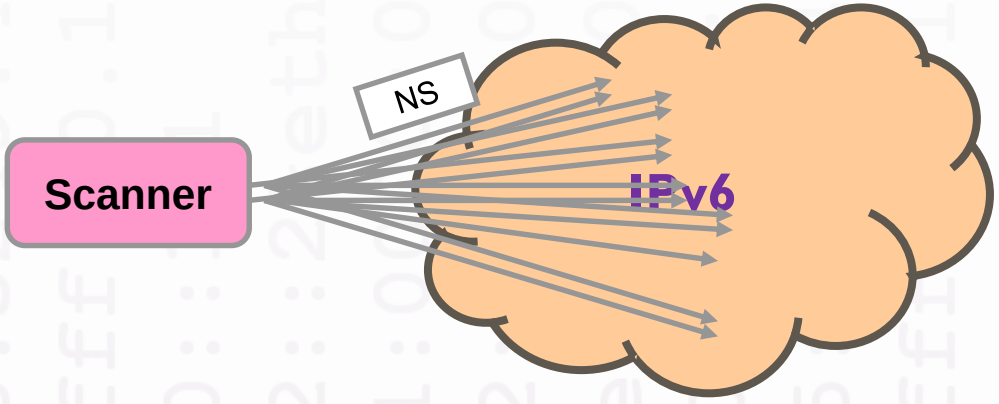
Scanning and Reconnaissance

- Scanning all addresses in IPv4 is easy
- IPv4 methods impractical for IPv6
  - No. of interface addresses 2^{64} = **18,446,744,073,709,551,616**
  - Would take **491,351** years on Gigabit Ethernet (no other traffic)
  - More intelligent, forms of reconnaissance are possible

RFC 7707

BETTER

IPv6 Prefix (64 bits)	**IPv6 Interface Identifier (64 bits)**



Length of NS frame = 840 bits
(including preamble and interframe gap)
Time to send NS on GbE = 0.00000084 seconds
Time to transmit all 2^{64} NS
= 1.54953×10^{13} seconds
= $1.54953 \times 10^{13} / 31536000 = 491351.6306$ years

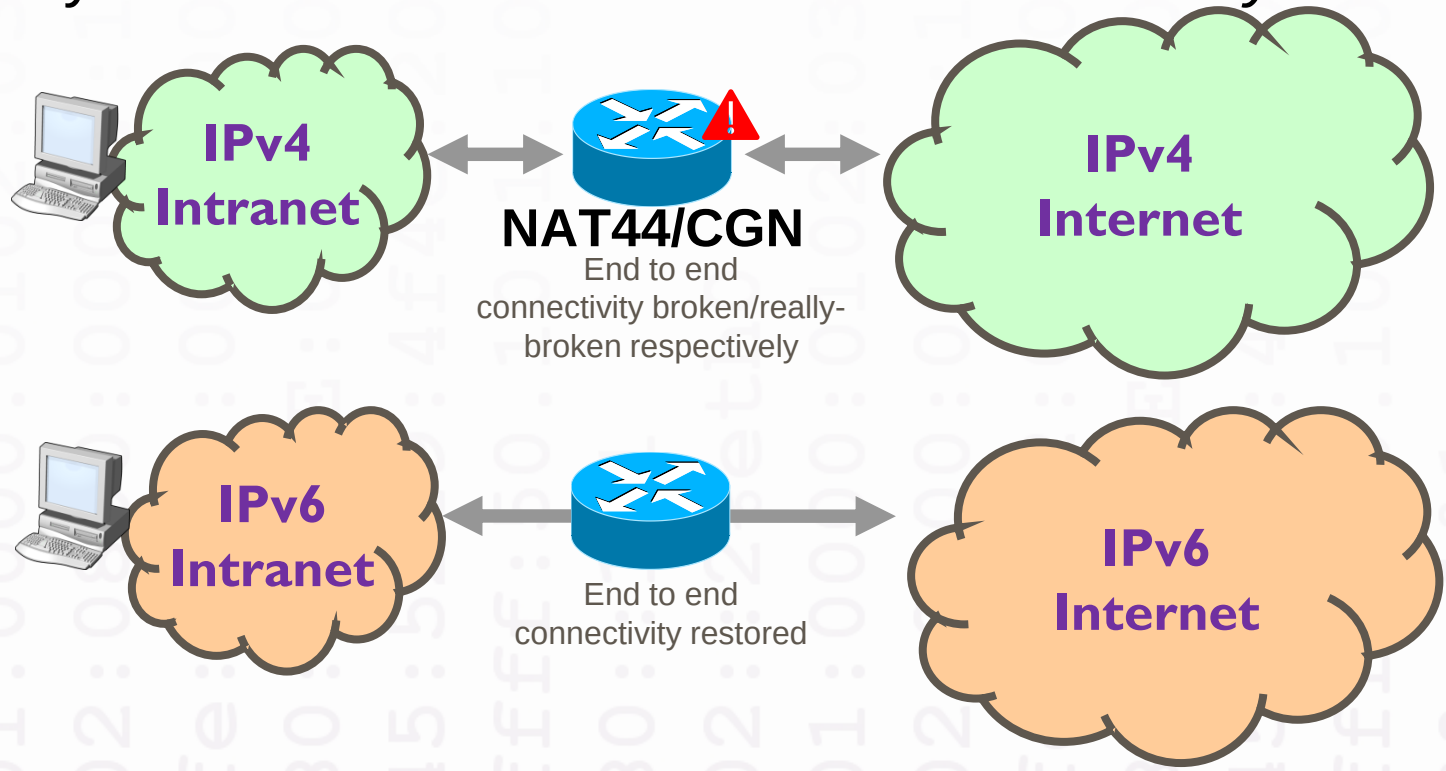
(assuming no other traffic or nodes in the subnet!)

Erion

End-to-End Transparency

NEW

- IPv6 restores end-to-end connectivity
- Global addresses everywhere: no NAT
- IPv6 security relies on *firewalls* not *broken connectivity*



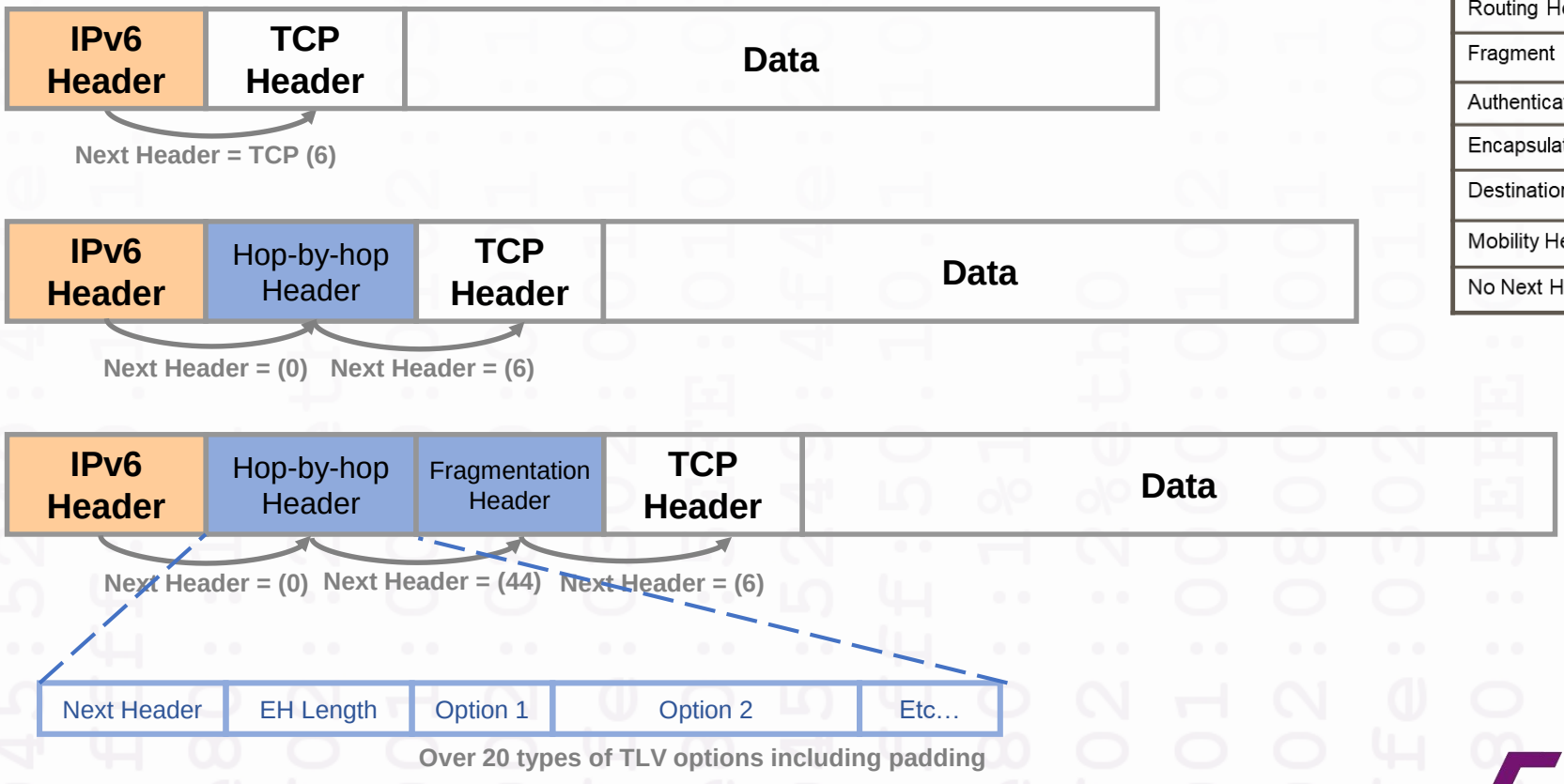
Erion

IPv6 Extension Headers

- Extension Headers (EHs) carry options
  - Many are extendable with complex formats and rules

NEW

Header Type
Hop-by-hop Options
Routing Header
Fragment Header
Authentication Header
Encapsulating Security Header
Destination Options
Mobility Header
No Next Header

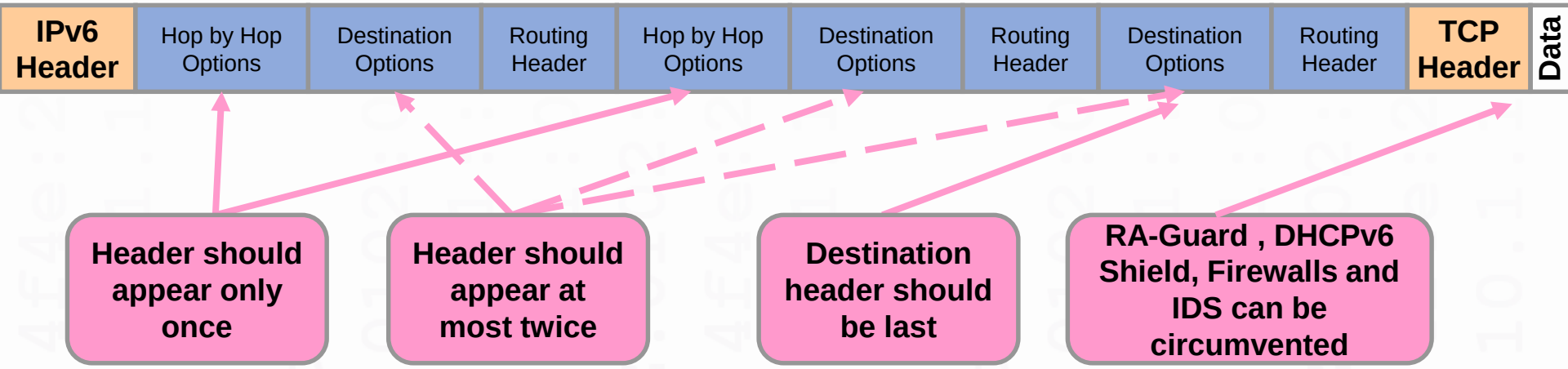


Erion

Extension Header Threats

- IPv6 places options in extension header chain
  - Originally no limit was placed on length of list

NEW



- Chain length makes deep packet inspection difficult
- Risk of abuse of length, order and duplication of headers
- Can be used to circumvent security mechanisms

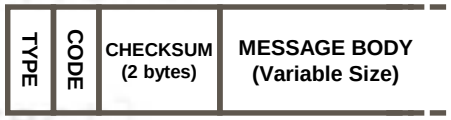
RFC2460
RFC6564
RFC7112

Erion

ICMPv6 Threats

NEW

```
Internet Control Message Pro
  Type: 135 (Neighbor solici
  Code: 0
  Checksum: 0x0074 [correct]
  Target: fe80::20c:29ff:feb5:
```



- More complex than ICMPv4
- More essential than ICMPv4
- Merges new and old features
- Requires ***new*** firewall policies
- Some messages ***must*** traverse firewalls
- Cannot secure most messages with IPsec

	Type	Message Type
ICMPv6 Error Messages	1	Destination Unreachable
	2	Packet Too Big
	3	Time Exceeded
	4	Parameter Problem
Ping	128	Echo Request
	129	Echo Reply
Multicast (MLD)	130	Multicast Listener Query
	131	Multicast Listener Report
	132	Multicast Listener Done
SLAAC	133	Router Solicitation
	134	Router Advertisement
Neighbor discovery, DAD, etc	135	Neighbor Solicitation
	136	Neighbor Advertisement
	137	Redirect Message
	138	Router Renumbering
	139	ICMP Node Information Query
	140	ICMP Node Information Response
	141	Inverse ND Solicitation
	142	Inverse ND Adv Message
Multicast (MLDv2)	143	Version 2 Multicast Listener Report
Mobile IPv6	144	ICMP Home Agent Address Discovery Request
	145	ICMP Home Agent Address Discovery Reply
	146	ICMP Mobile Prefix Solicitation
	147	ICMP Mobile Prefix Advertisement
	148	Certification Path Solicitation Message
	149	Certification Path Advertisement Message
	151	Multicast Router Advertisement
	152	Multicast Router Solicitation
	153	Multicast Router Termination
	154	Mobile IPv6 Fast Handovers FMIPv6
	155	RPL Control Message
	156	ILNPv6 Locator Update Message
6LowPAN	157	Duplicate Address Request
	158	Duplicate Address Confirmation
	159	MPL Control Message

RFC 4890

Erion

Neighbor Discovery (NDP)

RFC4861
RFC4862
RFC4311
RFC6583

Stateless address auto−configuration (SLAAC) NEW

- Router discovery
- Prefix discovery
- Parameter discovery
- Next−hop determination

NEW

Neighbor Discovery Protocol Threats

- Neighbor Cache poisoning
- Spoofing Duplicate Address Detection (DAD)
- Interfere with Neighbor Unreachability Detection (NUD)
- Rogue router
- Parameter Spoofing
- Bogus on-link prefixes
- Bogus address configuration prefixes
- Disabling routers
- Interfere with on-link determinations
- Forwarding loops
- Interfere with NDP Implementation
- Interfere with NDP router implementation from a remote site
- Replay attacks

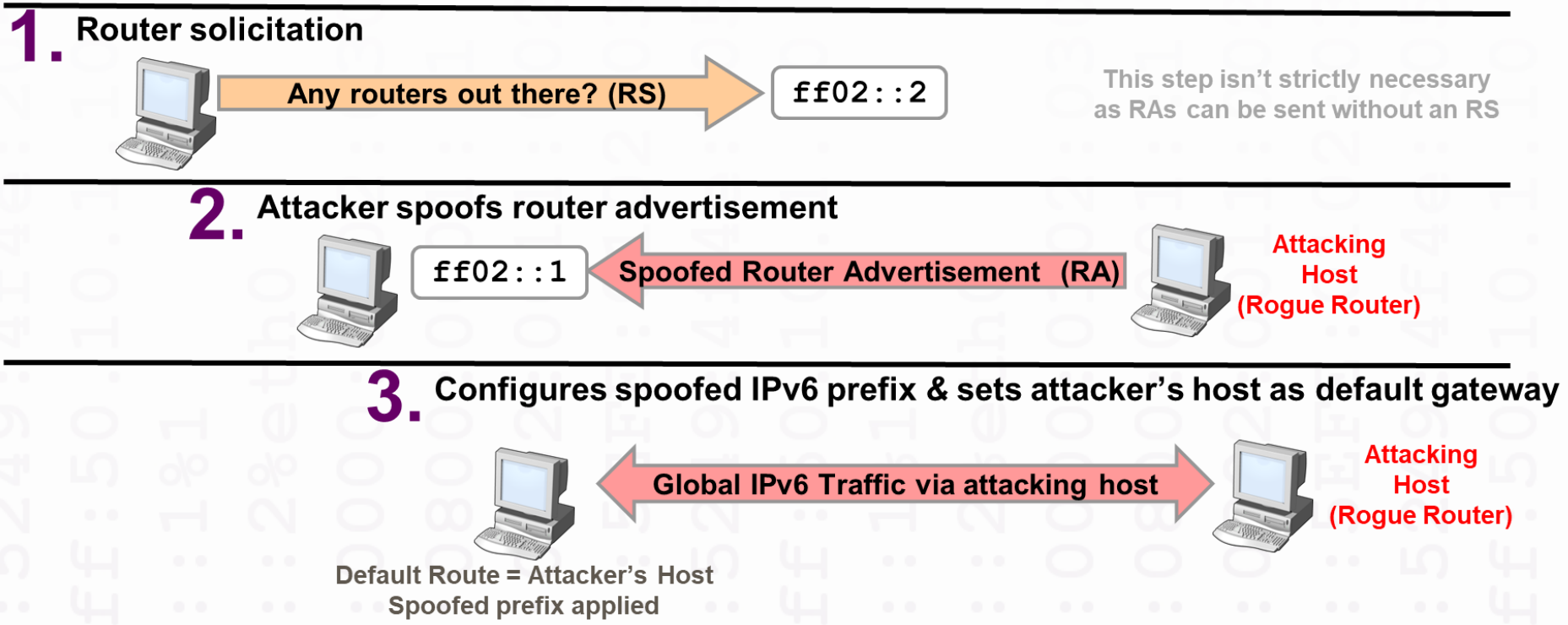
Address resolution DIFFERENT

- Neighbor unreachability detection (NUD)
- Duplicate address detection (DAD)

Erion

Example: Rogue Router

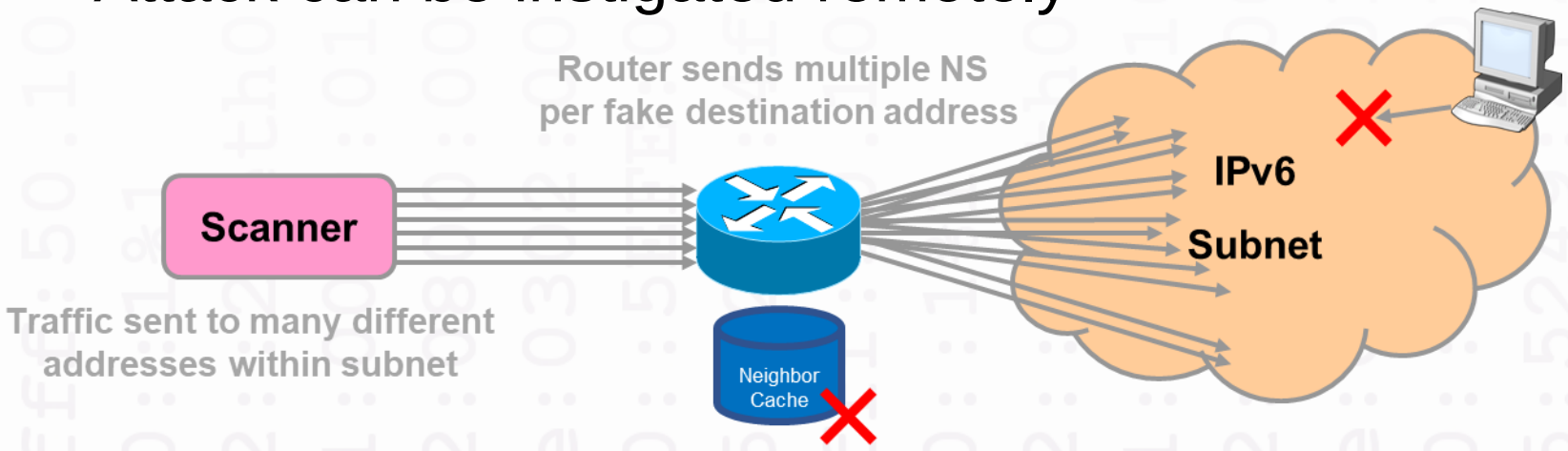
- Attacks: denial of service (DoS) and man-in-the-middle



Example: Remote NDP Attack

NEW

- IPv6 subnets are large
  - Addresses 2^{64} = 18,446,744,073,709,551,616
- NDP may be vulnerable to DoS attack
  - ND cache may be exhausted
  - Valid ND messages may be lost or they may expire
- Attack can be instigated remotely

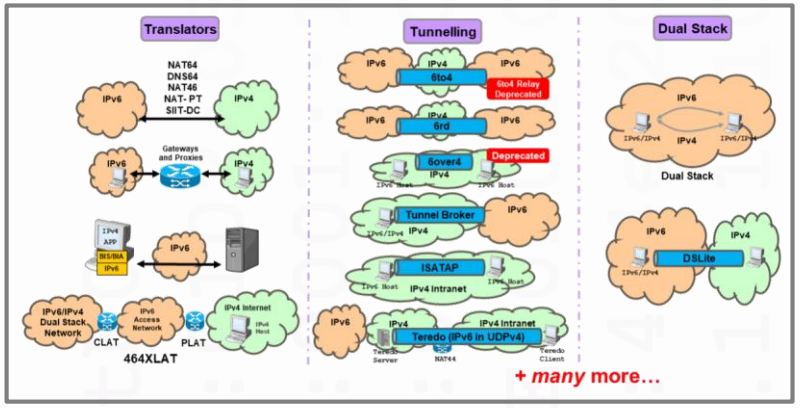


RFC 6583

Erion

Transition Mechanisms Threats

- Large number of mechanisms (~30)
- Complex interactions between IPv4 and IPv6
- Standard in many stacks
- Few have built-in security
- Complex address formats
- Each has many vulnerabilities
- Some can create backdoors



- All transition mechanisms are bad, some are necessary, you cannot simply ignore, you may have to use some

IPv6 Address Reputation

- Recording the reputation of 2^{128} addresses is impossible
- Attackers have a huge no. of source addresses to use
- Even recording prefix reputation is problematic

Number of /64s	Number of /48s	Number of /32s
18,446,744,073,709,551,616	281,474,976,710,656	4,294,967,296

  - It isn't quite as bad as the above. Only a part of the total address space has been reserved for public addresses. Out of this space only a part has been allocated to RIRs - never mind end users.
- Prefixes may be shared by many innocent parties
- Difficult for SMTP anti-spam measures (RDNSBL)
- Bad solutions can create new problems
- Also impacts analytics and forensics

Erion

Overview of IPv6 Security

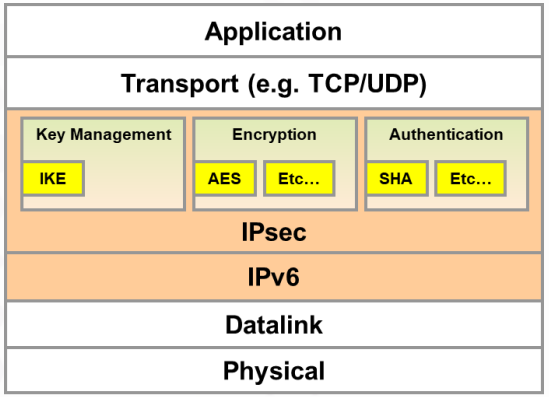
- Common Misconceptions about IPv6 Security
- IPv6 Threats and Vulnerabilities
- **IPv6 Security Features**
- The Future for IPv6 Security

Erion

IPv6 Security (IPsec)

- Built into and protects the network layer
- Allows for different security mechanisms and is extendable
- Two extension headers
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Interoperable
- Cryptographically based
- Was mandatory feature in IPv6 stacks
- Identical to IPv4 IPsec
- Cannot solve all security problems

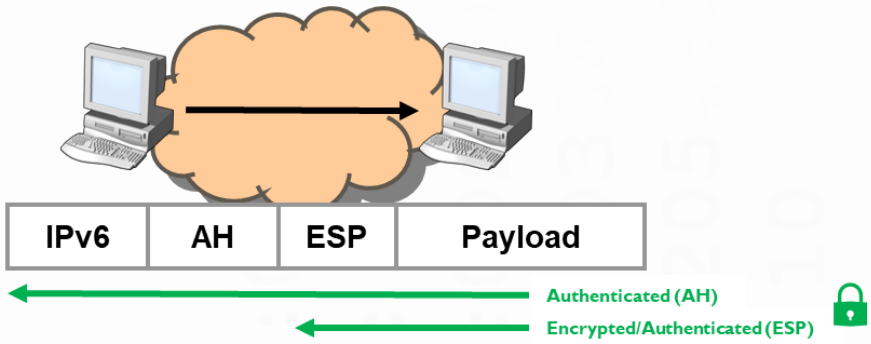
RFC 4301
RFC 4302
RFC 4303
RFC 4305
RFC 4306



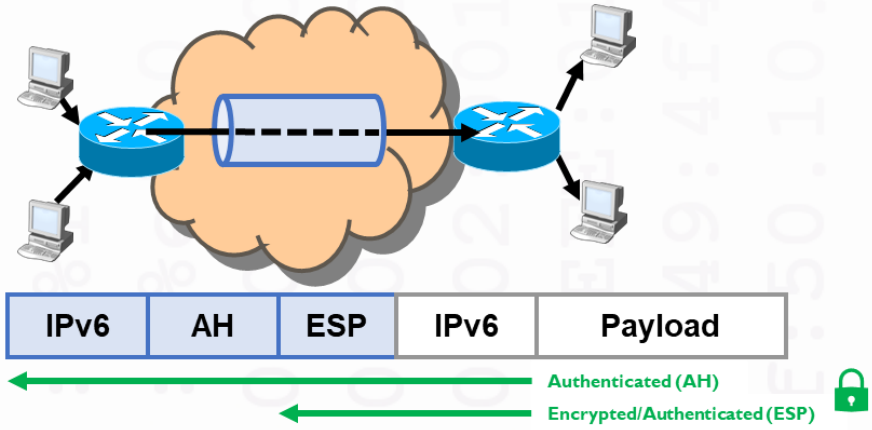
Erion

Transport and Tunnel Modes

- **Transport Mode**
  - Between two hosts
  - Rarer in IPv4 due to NAT44
  - More common in IPv6?



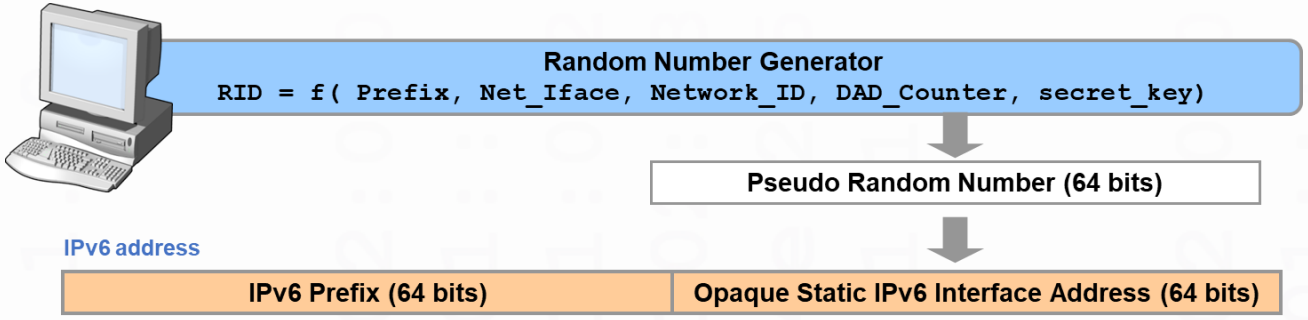
- **Tunnel Mode**
  - Security applied to tunnel
  - Between hosts or gateways
  - Secures whole IPv6 datagram
  - Used to create VPNs
  - Common in IPv4 due to NAT44



IPv6 Address Privacy

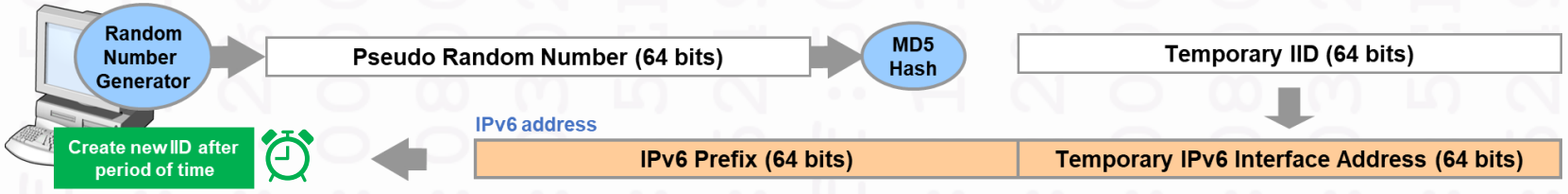
- **Opaque Static Addresses**
  - Avoids use of MAC address in IID (modified EUI-64)

RFC 7217



- **Privacy Addresses**
  - Temporary IID for client communications that changes with time

RFC4941

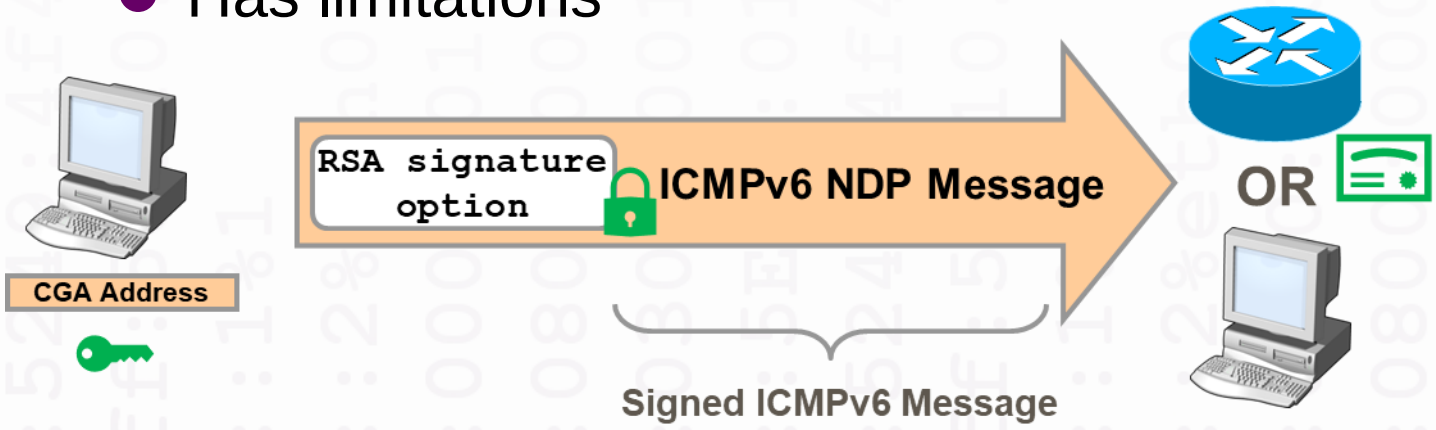


  - Has management implications

Erion

Secure Neighbor Discovery

- Can secure some Neighbor Discovery (ND) messages
- May form part of PKI or use local trust anchor
- Uses Cryptographically Generated Addresses (CGAs)
  - CGAs bind the IID to a public key
- Not widely available on all platforms
- Has limitations



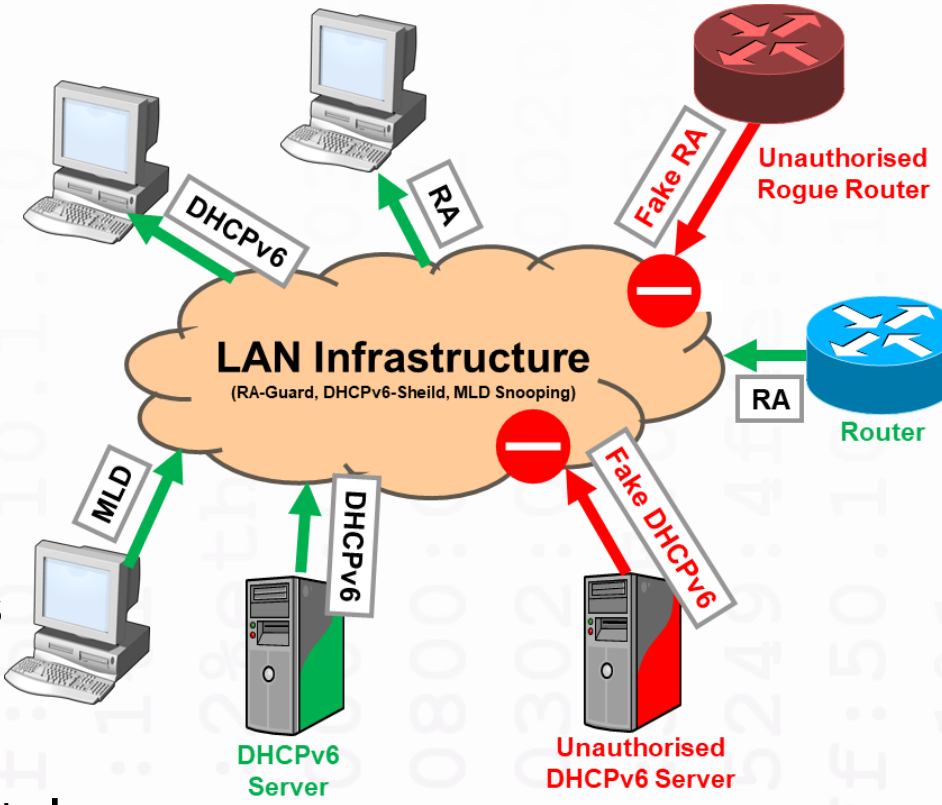

```
Internet Protocol Version 6, Src: fe8
Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x5862 [correct]
    Cur hop limit: 64
  ▸ Flags: 0x20
    Router lifetime (s): 30
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ▸ ICMPv6 Option (Prefix information
  ▾ ICMPv6 Option (Source link-layer ad
      Type: Source link-layer address
      Length: 1 (8 bytes)
      Link-layer address: Vmware_4e:25
  ▾ ICMPv6 Option (CGA)
      Type: CGA (11)
      Length: 24 (192 bytes)
      Pad Length: 1
      Reserved
    ▸ CGA: d862adb99efe5b68a9a0e431563
      Padding
  ▾ ICMPv6 Option (Timestamp)
      Type: Timestamp (13)
      Length: 2 (16 bytes)
      Reserved
      Timestamp: Dec 14, 2016 12:43:05
  ▾ ICMPv6 Option (RSA Signature)
      Type: RSA Signature (12)
      Length: 19 (152 bytes)
      Reserved
      Key Hash: a0828691967292db133b6b
      Digital Signature and Padding
```

RFC3971
RFC6494
RFC6495

Erion

IPv6 LAN Security Features

- **Neighbor Discovery Inspection**
  - Validation of NDP messages
- **RA-Guard**
  - Validation and control of RAs
- **DHCPv6-Shield**
  - Validation/control of DHCPv6
- **MLD Snooping**
  - Multicast LAN performance
  - Limits some multicast attacks



- Usually implemented in switches
- Can be circumvented

Erion

Attacking Security Features

- RA-Guard, MLD-Snooping, DHCPv6-Shield and Neighbor Discovery Protocol Inspection can all be circumvented - easily
- **Extension headers** make packet inspection difficult

- Attacks can be hidden in **second fragment**

- Recent standards address these problems
  - Constrain the use of extension headers
  - Restrict the fragmentation of certain protocols
  - Verify your equipment adheres to current standards

RFC7112

RFC6980

Erion

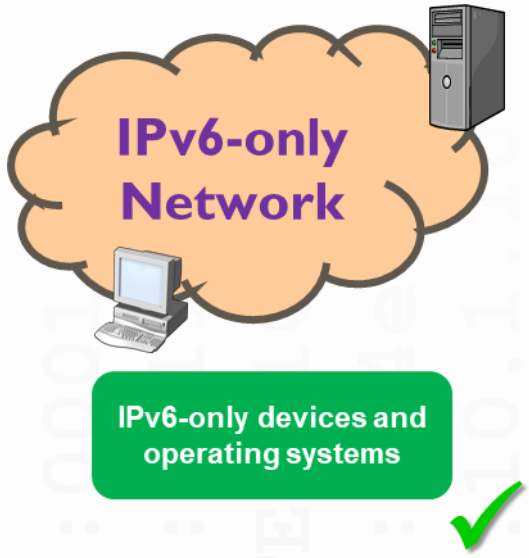
Overview of IPv6 Security

- Common Misconceptions about IPv6 Security
- IPv6 Threats and Vulnerabilities
- IPv6 Security Features
- **The Future for IPv6 Security**

The Future of IPv6 Security

IPv6-only networks

- No further need to support IPv4
- No IPv4 vulnerabilities
- No transition mechanisms vulnerabilities
- Make best use of IPv6 security features
- Reduced operational costs



Erion

Conclusions

- IPv4-only networks are historic
- IPv6 should already form a part of your security policy
- IPv6 security introduces many new vulnerabilities and features
- IPv6-only networks will have fewer vulnerabilities
- Legacy IPv4 thinking is a risk; staff IPv6 competency is crucial

Erion

Questions and Discussion

Thank you for listening

Further Information

Erion	http://www.erion.co.uk
IPv6 Training	http://www.ipv6training.com
IPv6 Consultancy	http://www.ipv6consultancy.com
IPv6 Blog	http://www.ipv6consultancy.com/ipv6blog

Erion

Profile: David Holder

- CEO & Chief Consultant Erion
- Author of numerous reports and whitepapers
- Regular speaker on IPv6
- Extensive experience of IPv6 spanning over 20 years
- Chairman of IPv6 Task Force Scotland