IPv6 Security Fundamentals

UK IPv6 Council January 2018

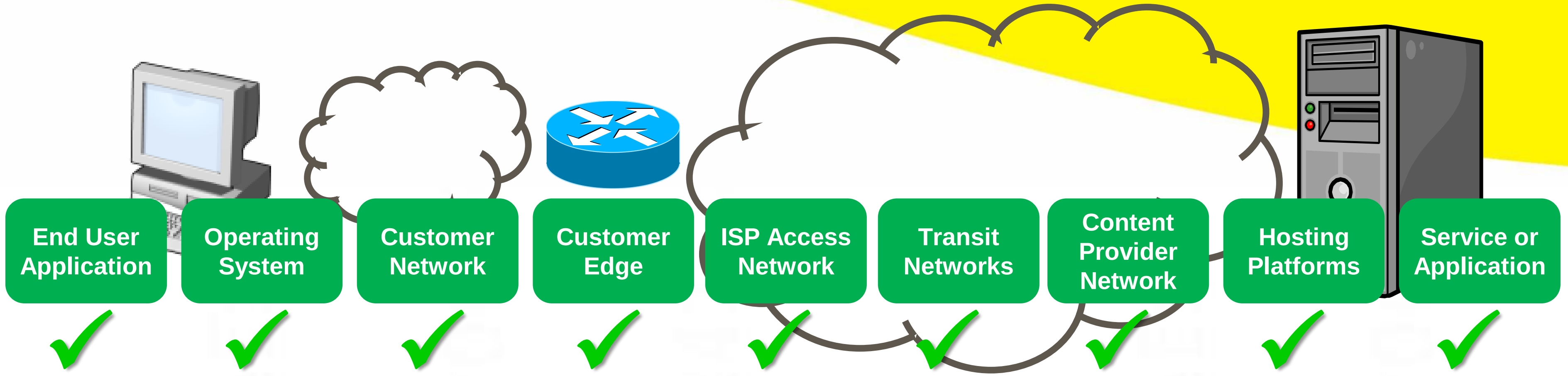
Dr David Holder CEng FIET MIEEE

david.holder@erion.co.uk

IPv6 Security Fundamentals

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

Why Does IPv6 Security Matter?



- Dual stack users: **75%** of traffic is over IPv6
- Over **18%** of users have IPv6 connectivity
- Over **50%** of top websites are IPv6 enabled
- Annual **doubling** of IPv6 users
- IPv6 is **10-15% faster** than IPv4
- **Almost 100% of nodes are IPv6 capable**

IPv6 Security Fundamentals

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

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

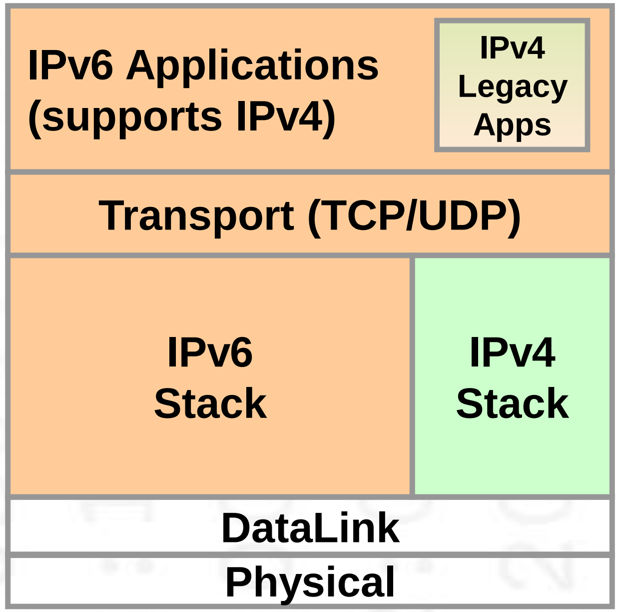
More about why people think this later, but first the truth…

Today’s Reality: IPv6 Dual Stacks

- Today’s operating systems and devices are all dual stack
- IPv6 on by default
- Even IPv4 networks are built on IPv6 dual stacks
- Combined IPv4/IPv6 vulnerability surface

Dual Stack Implications

- Comparing IPv4 and IPv6 security is irrelevant
- Dual stack is everywhere even without deploying IPv6
- IPv6 is already in your network today
- Turning it off is the wrong thing to do



- Combined IPv4/IPv6 vulnerability surface
  - Attackers will choose weakest link
  - DoS possible due to shared resources
  - Complexity more than doubled

- So, secure your network against IPv6 vulnerabilities now

  (Ideally you should have done this over decade ago)

The Third Big Misconception

3. IPv6 is IPv4 with longer addresses ✕

Prefix (64 bits)	Interface ID (64 bits)

- **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

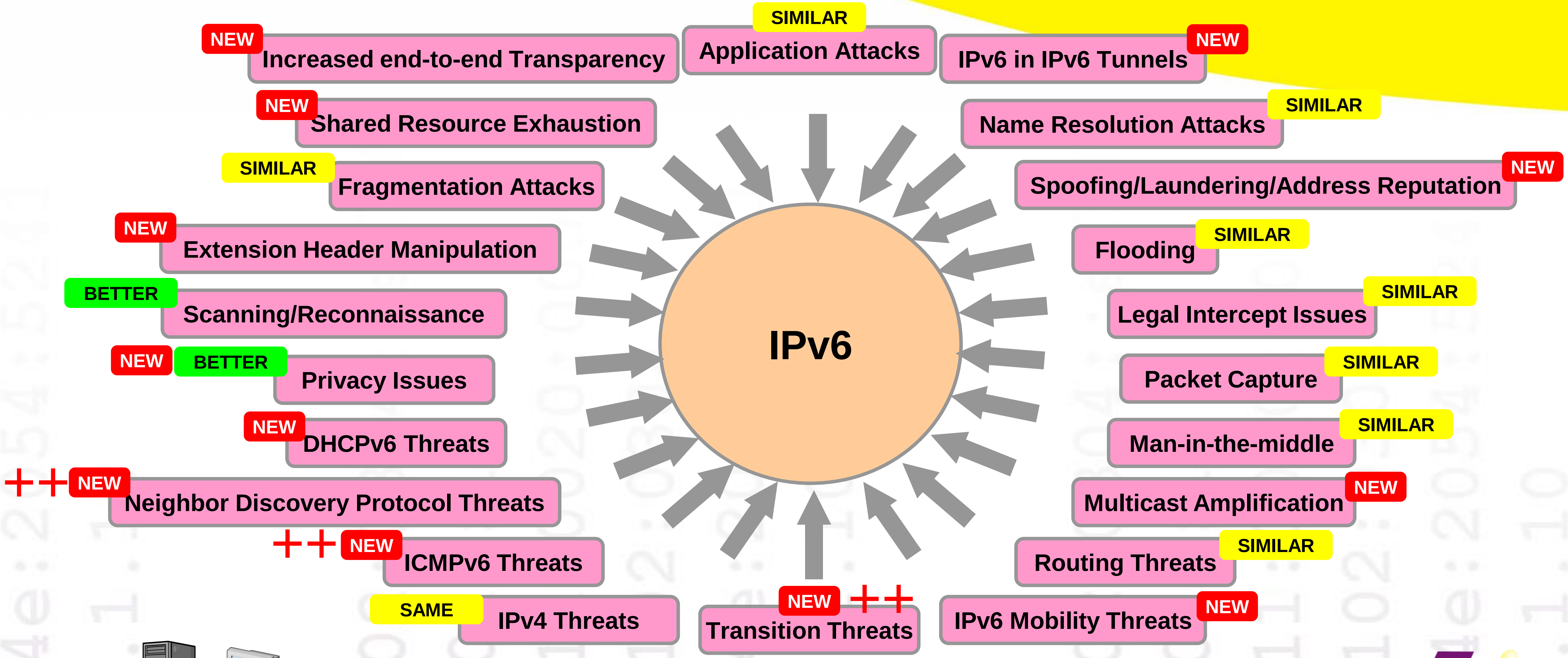
IPv6 Security Fundamentals

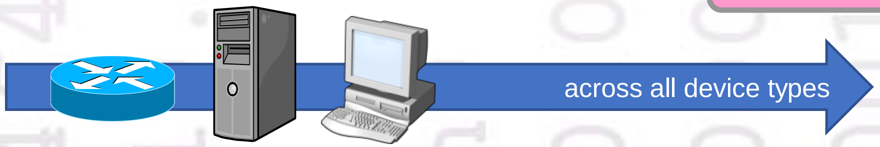
- Common Misconceptions about IPv6 Security
- **IPv6 Threats and Vulnerabilities**
- IPv6 Security Features
- The Future for IPv6 Security

IPv6 Security: The Problems

- **Complexity**
  - *Lots* of changes and new features
  - IPv6 is flexible and extendable
- **Shares resources**
  - IPv4 and IPv6 share resources
- **IPv4 and IPv6 coupling**
  - Transition mechanisms
- **Standards evolving over time**
  - Presents a moving target
- **Staff competency in IPv6**
  - Legacy IPv4 thinking

The IPv6 Vulnerability Surface





IPv6 Threats: Reality Check

- **IPv6 firewalls/security**
  - Now common and on by default
- **Common threats**
  - Many vulnerabilities are common to both IPv4 and IPv6
- **Common attack vectors**
  - Different vulnerabilities often have common attack vectors
- **Many vulnerabilities are not new**
  - We already have mitigation strategies for many threats
- **Double standards**
  - IPv6 criticised for things that are ignored in IPv4

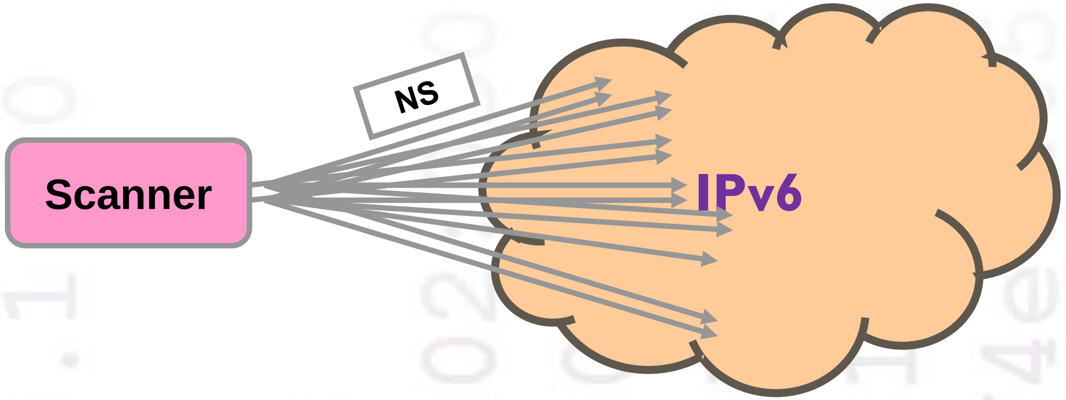
Scanning and Reconnaissance

RFC 7707

BETTER

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

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



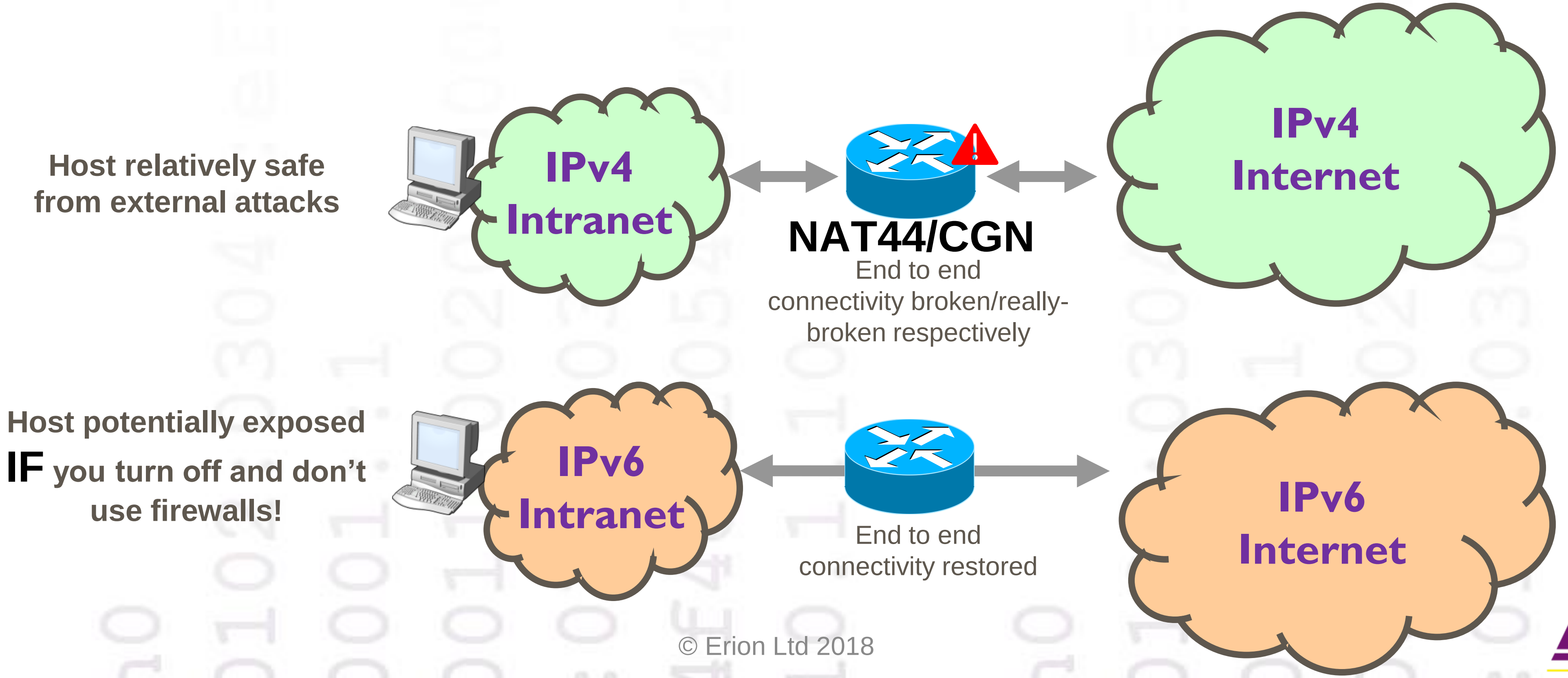

```
Length of NS frame (including preamble and interframe gap) = 840 bits
Time to send NS on GbE = 0.00000084 seconds
Time to transmit all 2^64 NS = 1.54953 x 10^13 seconds
= 1.54953 x 10^13/31536000 = 491351.6306 years

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

End-to-End Transparency

NEW

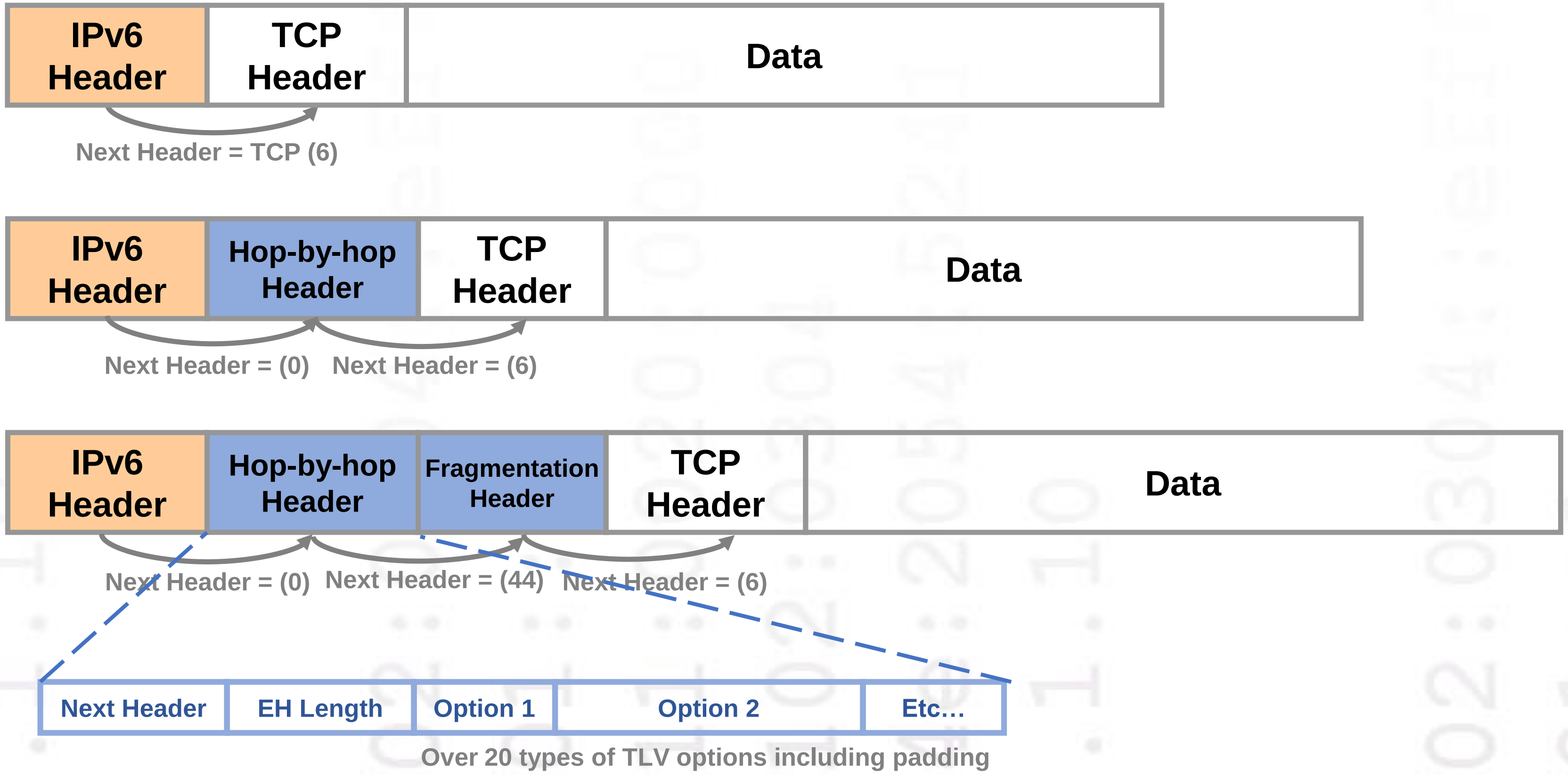
- IPv6 restores end-to-end connectivity
- Global addresses everywhere: no network address translation
- IPv6 security relies on *firewalls* instead of *broken connectivity*



IPv6 Extension Headers

NEW

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

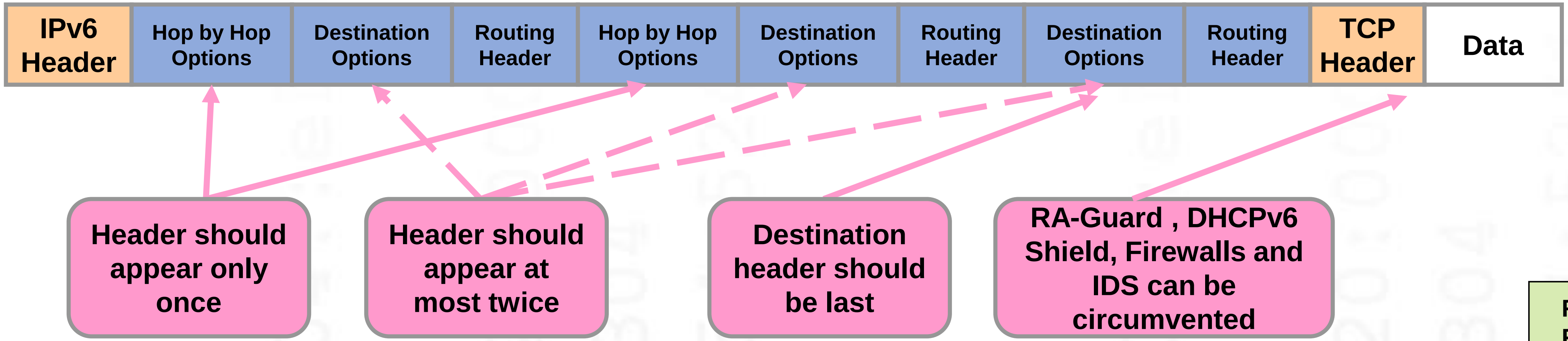


Header Type	Next Header
Hop-by-hop Options	0
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulating Security Header	50
Destination Options	60
Mobility Header	135
No Next Header	59

IPv6 Extension Header Threats

NEW

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



RFC2460
RFC6564
RFC7112

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

ICMPv6 Threats

NEW

- 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

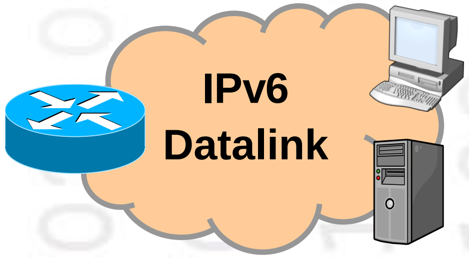
Address resolution DIFFERENT

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

NEW

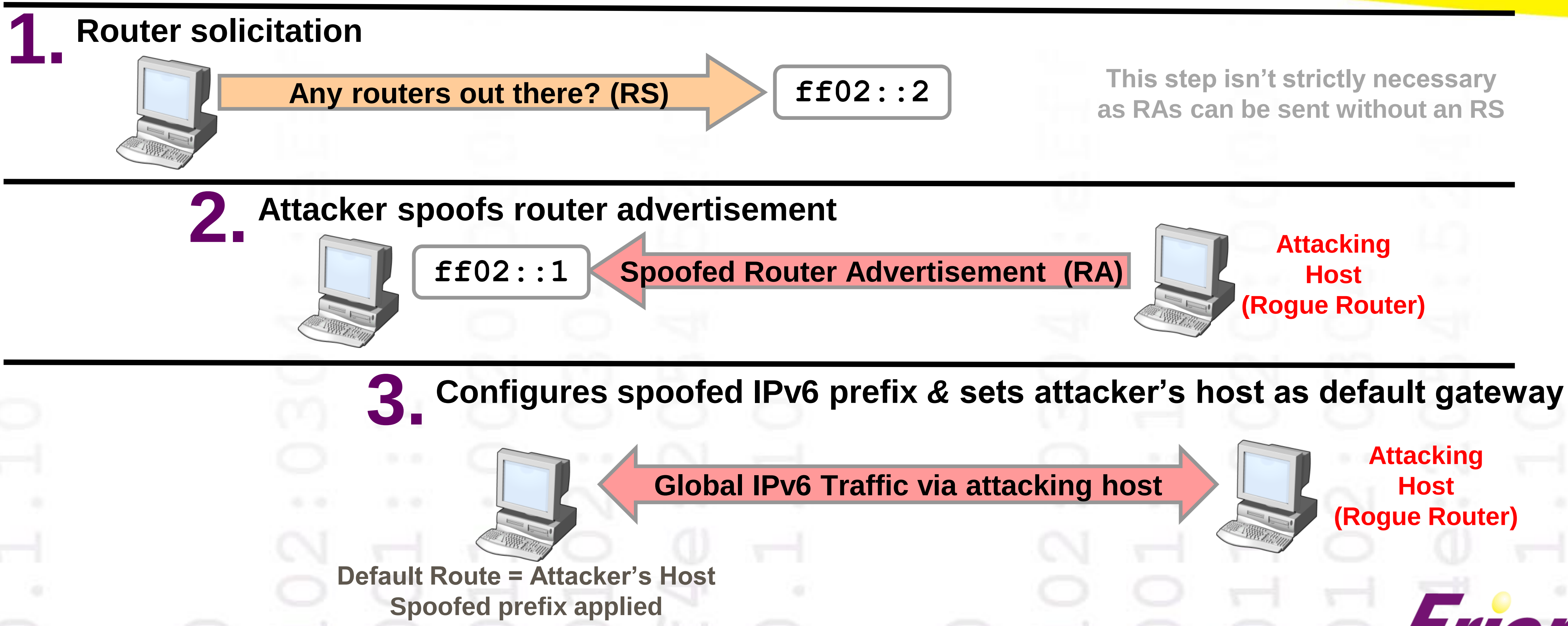
Neighbor Discovery Protocol Threats

- 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



Example: Rogue Router

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

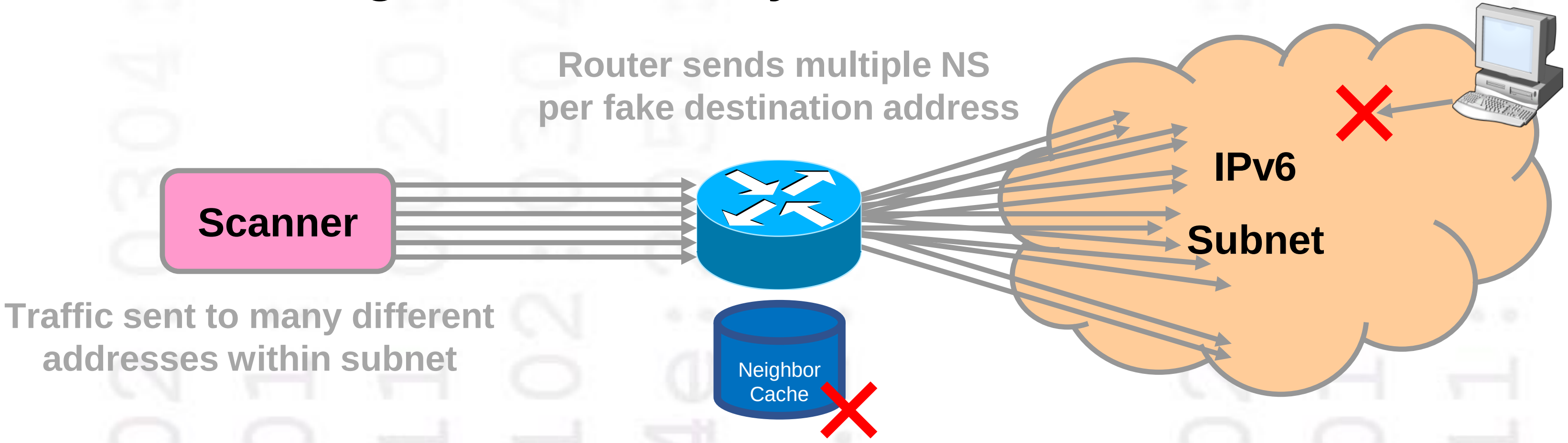


Example: Remote NDP Attack

RFC 6583

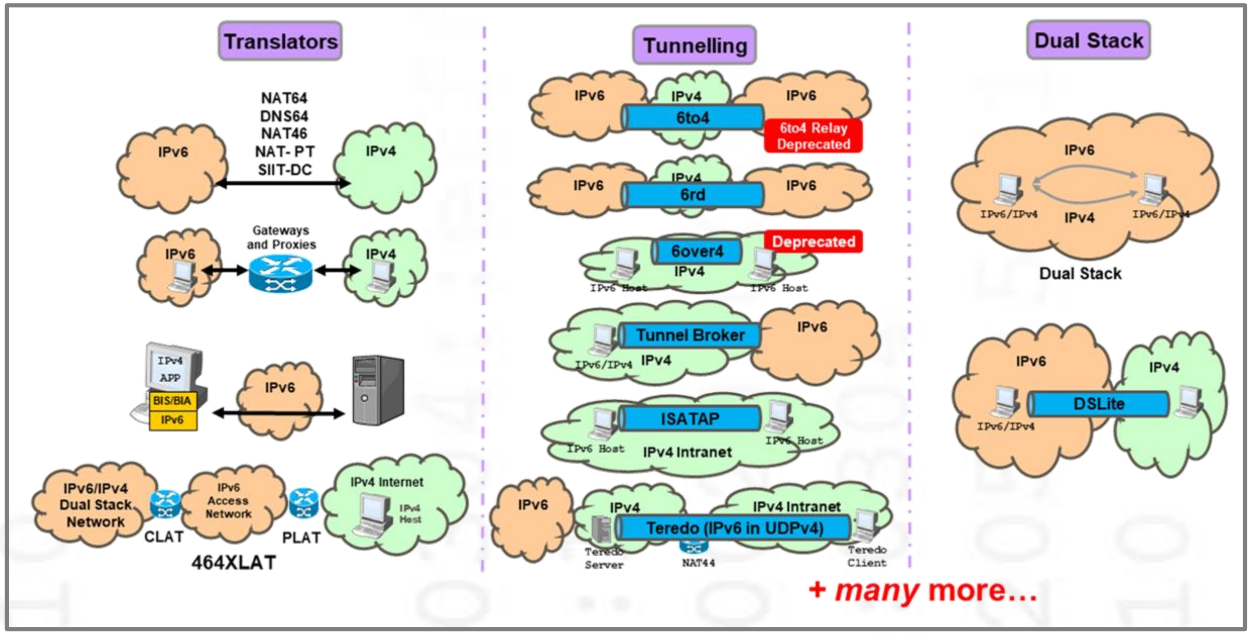
NEW

- IPv6 subnets are large
  - Interface 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



Transition Mechanisms Threats

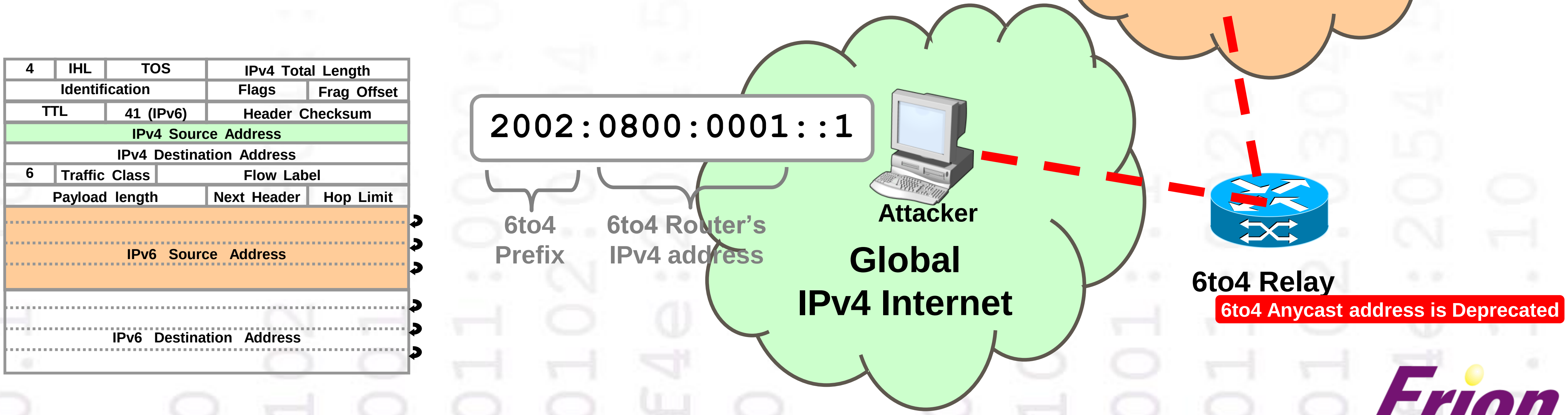
- Large number of mechanisms (~30)
- Complex interactions between IPv4 and IPv6
- Standard in many stacks
- Few have built-in security
- Complex address formats
- Each has many vulnerabilities
- Some can create backdoors



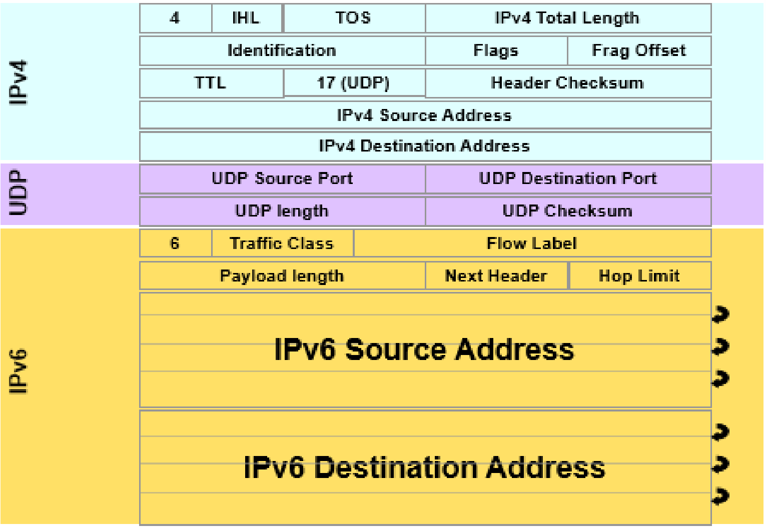
- All transition mechanisms are bad, some are necessary, you cannot simply ignore, you may have to use some

Example 6to4 Threat

- Spoofed traffic injected into IPv6 network from IPv4 internet
  - IPv4 Source = Spoofed
  - IPv4 Destination = 6to4 Relay
  - IPv6 Source = Spoofed
  - IPv6 Destination = Victim
- 6to4 treats IPv4 internet as single subnet

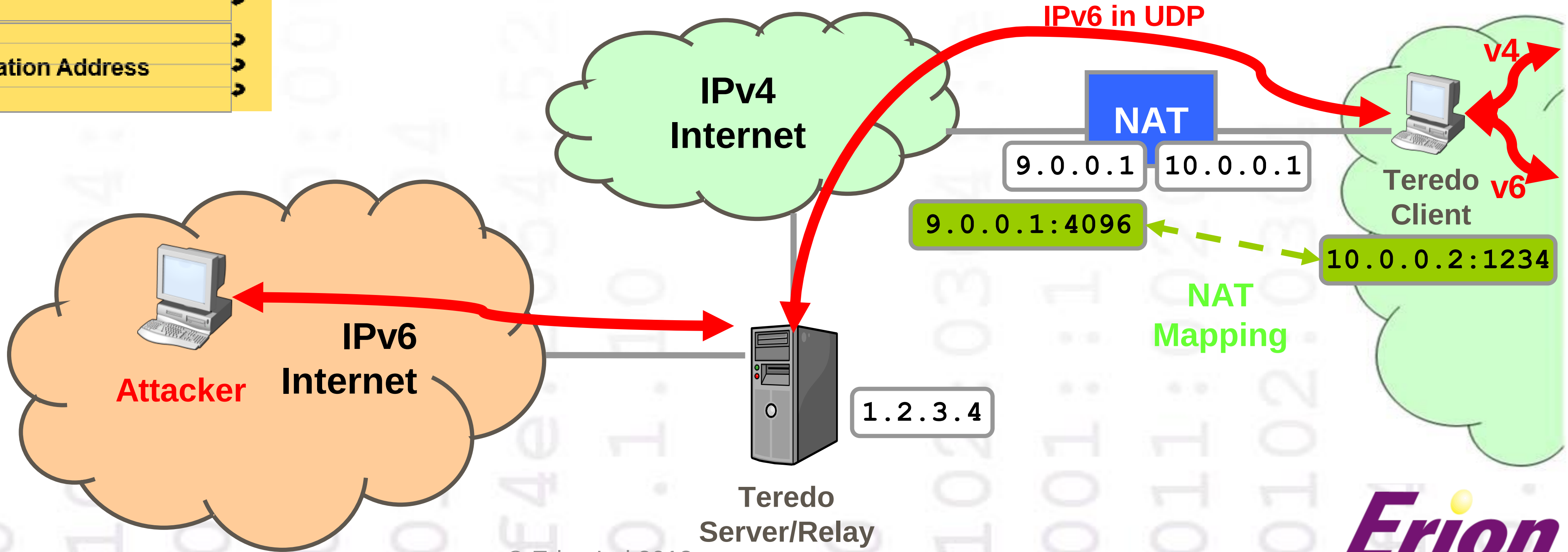


Teredo Threat Example



2001:0000:0102:0304::efff:f6ff:fffe

- Teredo 32 bit Prefix
- IPv4 address of Teredo Server
- UDP mapped Port (4096) XORed with FFFF
- XOR of FFFF:FFFF with 0900:000 (IPv4 mapped address)



IPv6 Address Reputation

- Recording the reputation of all 2^{128} addresses is impossible
- Attackers have a huge number 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
- Particularly difficult for SMTP anti-spam measures (RDNSBL)
- Bad solutions can create new problems

Erion

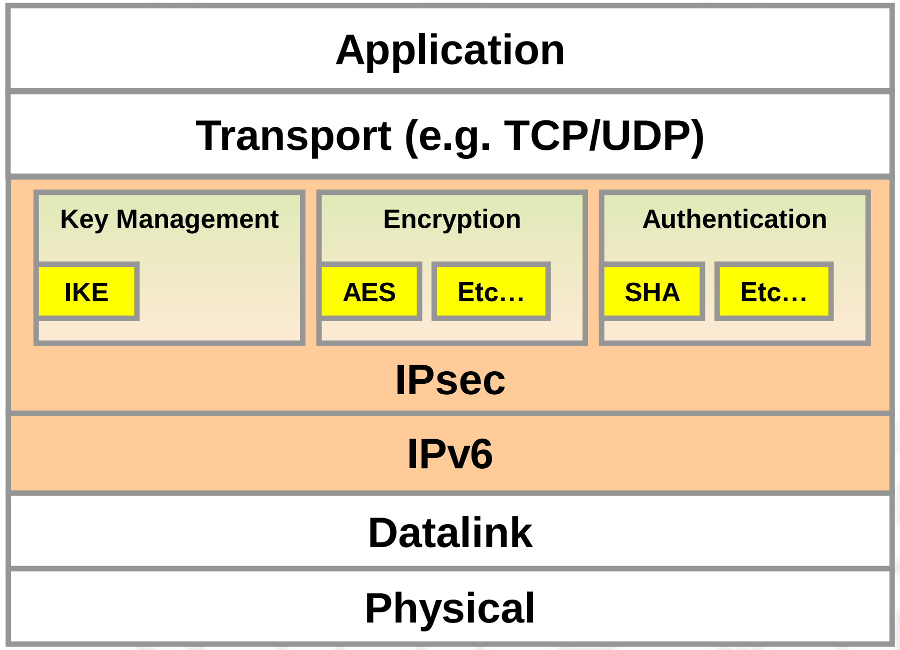
IPv6 Security Fundamentals

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

IPv6 Security (IPsec)

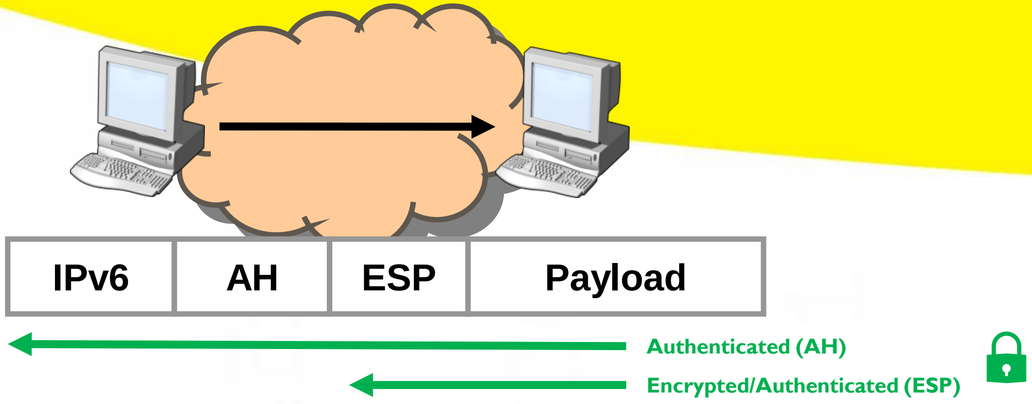
RFC 4301
RFC 4302
RFC 4303
RFC 4305
RFC 4306

- 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

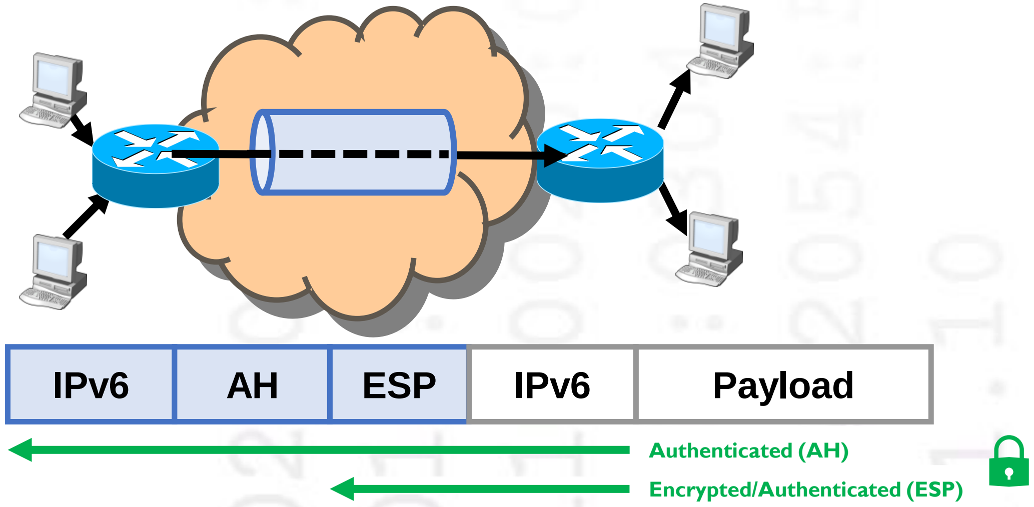


Transport and Tunnel Modes

- **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

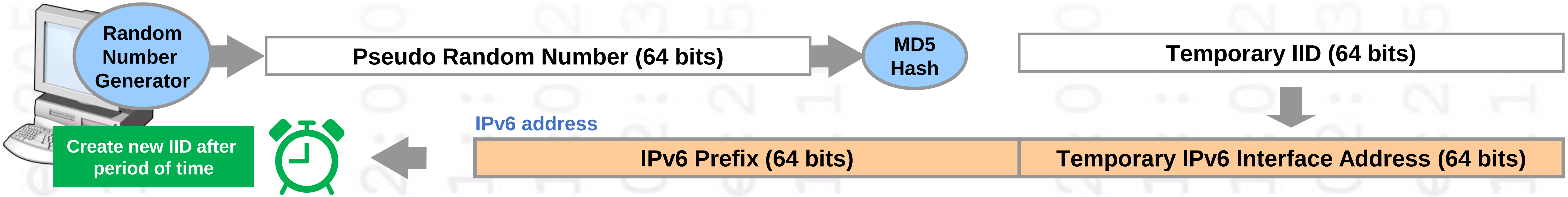


Erion

Privacy Addresses in IPv6

RFC4941

- Alternative to modified EUI-64 Interface Identifiers (IIDs)
- Avoids exposing MAC address in IPv6 addresses
- Address is used for *client* connections
- Temporary address is refreshed after a *short* period of time
- Makes harvesting addresses for future attacks difficult
- Has management implications



Opaque Static Addresses

RFC 7217

- Avoids use of MAC address in IID (modified EUI-64)
- Avoids exposing MAC address in IPv6 address
- Generates a predictable IID
- IID does not change with time
- IID is different for each network and prefix

Random Number Generator

`RID = f( Prefix, Net_Iface, Network_ID, DAD_Counter, secret_key)`

↓

Pseudo Random Number (64 bits)

↓

IPv6 address

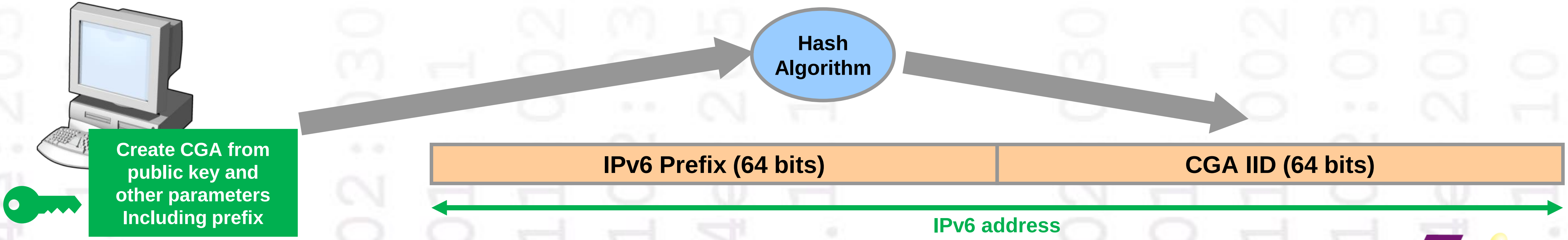
IPv6 Prefix (64 bits)	Opaque Static IPv6 Interface Address (64 bits)

Erion

Cryptographically Generated Addresses (CGA)

RFC3972
RFC4581
RFC4982

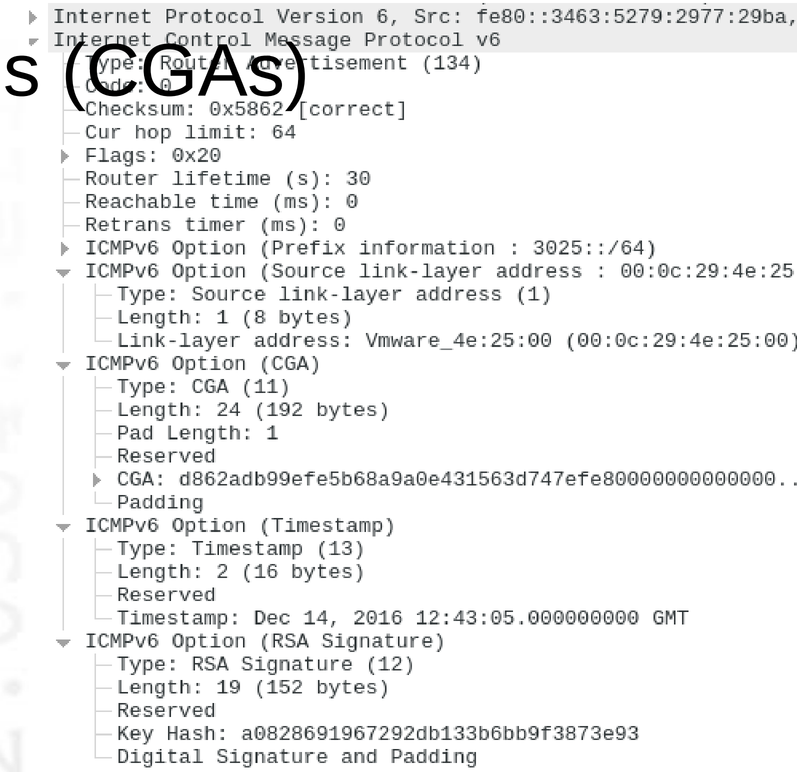
- Used to prove the ownership of an IPv6 address
- Binds IPv6 interface ID (IID) to a public key
- Is created from a hash of public key and other parameters
- CGA is verified by calculating the hash and comparing with IID
- Does not require public key infrastructure (PKI)

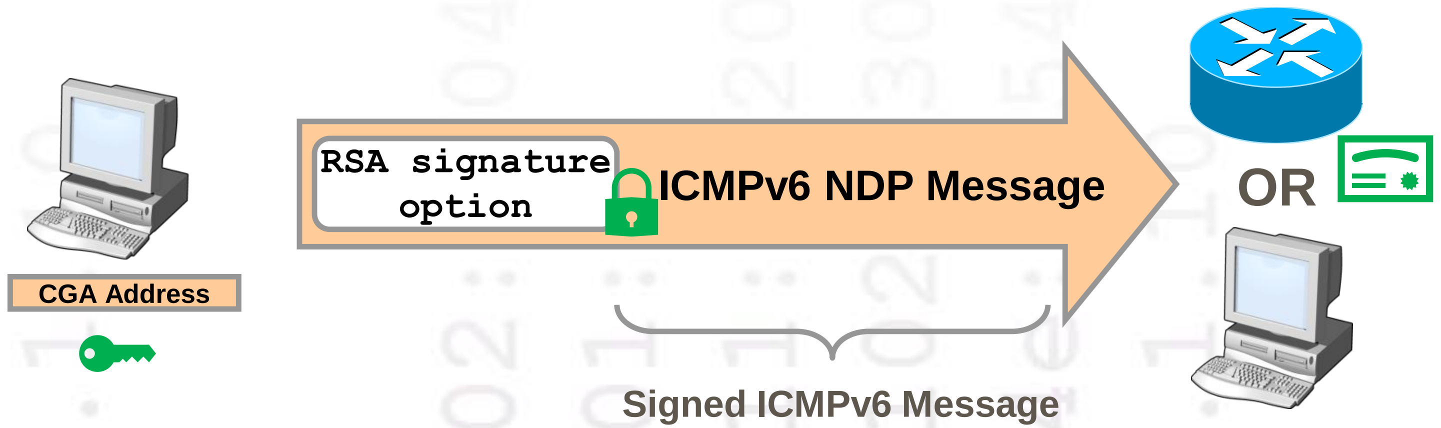


Secure Neighbor Discovery (SeND)

RFC3971
RFC6494
RFC6495

- Secures some Neighbor Discovery (ND) messages
- Can form part of PKI or use local trust anchor
- Uses Cryptographically Generated Addresses (CGAs)
- Not widely available on all platforms
- Has limitations



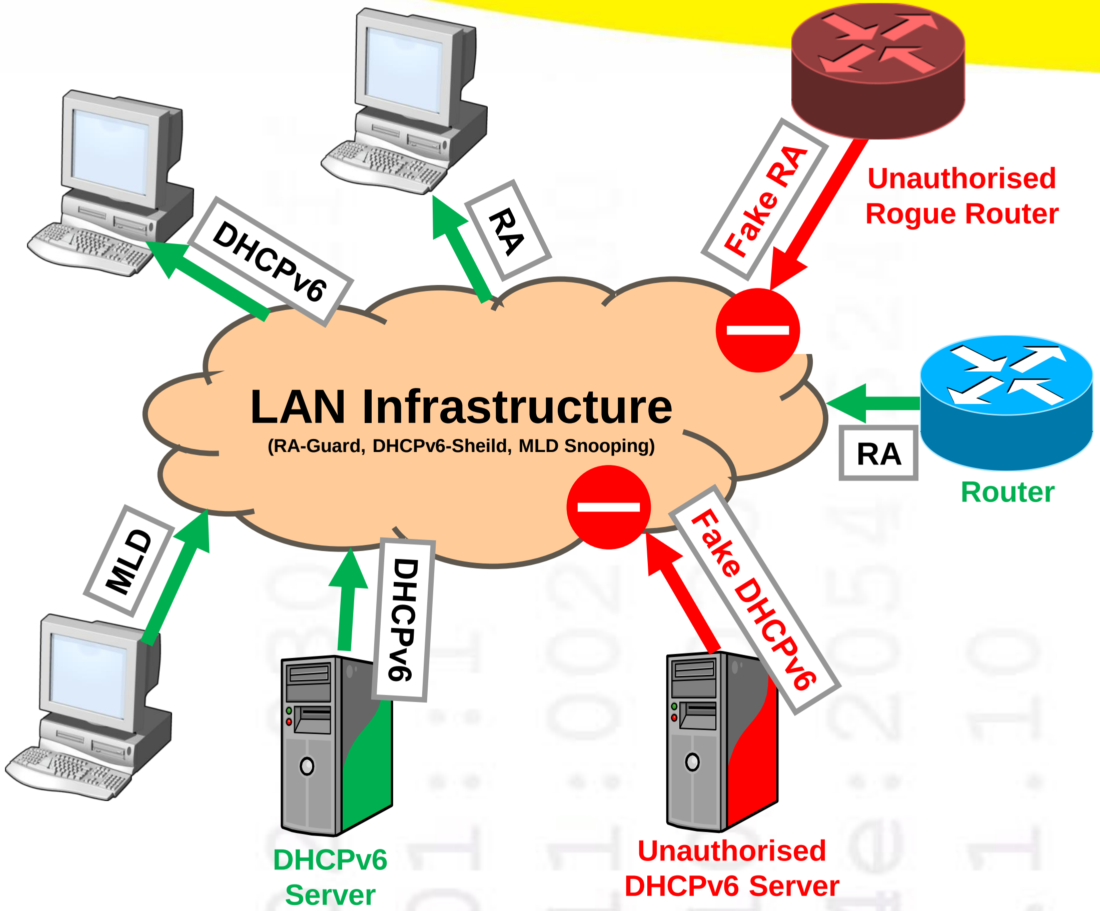


Erion

IPv6 LAN Security Features

- **RA-Guard**
  - Validation and control of RAs
- **DHCPv6-Shield**
  - Validation and control of DHCPv6
- **Neighbor Discovery Inspection**
  - Validation of NDP messages
- **MLD Snooping**
  - Improves multicast LAN performance
  - Can limit certain multicast attacks

- Usually implemented in switches
- Can be circumvented



Attacks Against Security Features

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

IPv6	EH1	EH2	ICMPv6 Fake RA

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

Fragment 1

IPv6	Frag EH	EHs

Fragment 2

IPv6	Frag EH	EHs	ICMPv6 Attack

- 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

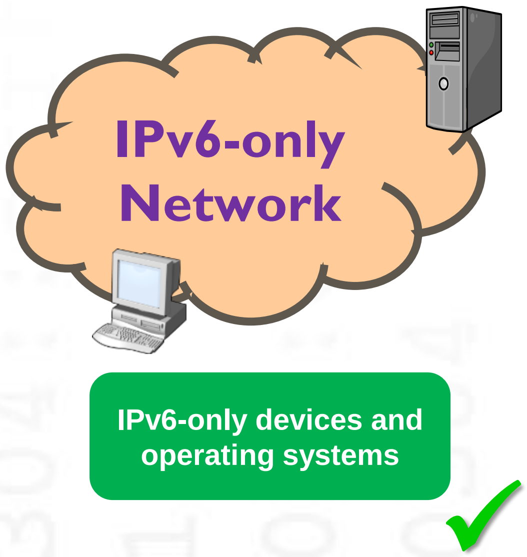
IPv6 Security Fundamentals

- 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



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

Any Questions?

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

IPv6 Training

19th Jan 2018	*Implementing and Securing IPv6*
6th Feb 2018	*IPv6 Forensics* **NEW**

Closed on-site courses available worldwide

Many other IPv6 courses and IPv6 security courses available

Profile: David Holder

- CEO and Chief Consultant Erion Ltd
- Author of numerous reports and whitepapers
- Chairman of IPv6 Task Force Scotland
- Regular speaker on IPv6
- Extensive experience of IPv6 spanning over 19 years