secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

Safer Six
IPv6 Security in a Nutshell

Johanna Ullrich

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfw
Bundesministerium für
Wissenschaft, Forschung und Wirtschaft

Christian Doppler
Forschungsgesellschaft

FFG

FWF

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

secure
sba-research.org

secure
sba-research.org

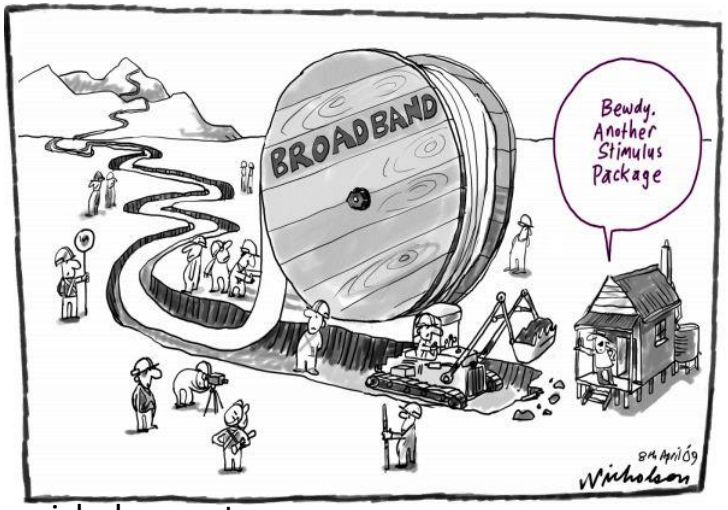
secure
sba-research.org

„I think there is a world market
for maybe five computers“

Thomas Watson

Reasons

connect.de



nicholsoncartoons.com.au

networkworld.com

Pattern	Address class	Range
0	A	0 – 127
10	B	129 – 191
110	C	192 – 223
1110	D	224 – 239
1111	E	240 – 255

„Computers in the future may [...]
weigh only 1.5 tons“

Popular Mechanics, 1949

in *Workshop on Offensive Technologies, 2014*

IPv6 Security: Attacks and Countermeasures in a Nutshell

Johanna Ullrich, Katharina Krombholz, Heidelinde Hobel, Adrian Dabrowski, Edgar Weippl
SBA Research
Vienna, Austria
Email: (1stletterfirstname)(lastname)@sba-research.org

***Abstract*—The history of computers is full of underestimation: 640 kilobyte, 2-digit years, and 32-bit Internet addresses. IPv6 was invented to overcome the latter as well as to revise other drawbacks and security vulnerabilities of its predecessor IPv4. Initially considered the savior in terms of security because of its mandatory IPsec support, it turned out not to be the panacea it was thought to be. Outsourcing security to IPsec but eventually removing it as well as other design decisions led to a number of vulnerabilities. They range from the already known spoofing of answers to link-layer address requests to novel possibilities regarding node tracking. In an effort to fix them, a vast amount of updates have been introduced.**

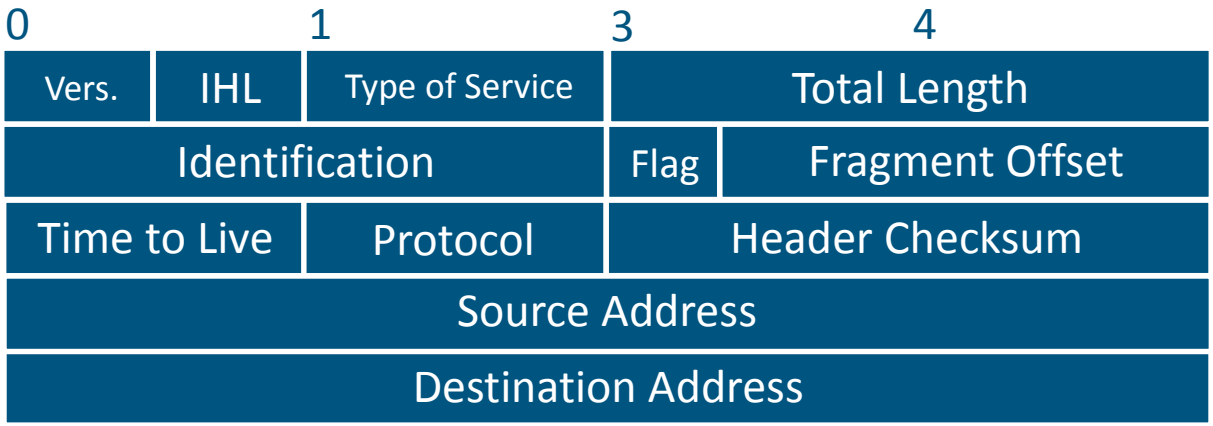
In this paper, we discuss security and privacy vulnerabilities with regard to IPv6 and their current countermeasures. In a

in various scientific papers, *Requests for Comments* (RFCs), videos and blogs. It is, therefore, a time-consuming and tedious task to collect all the findings and to obtain a comprehensive understanding of this topic. In addition to scientific work, we included non-scientific contributions from hacker blogs to complete our systematization with security challenges that were detected in the wild. The overall goal of this paper is to summarize and systematize the IPv6 vulnerabilities as well as the associated countermeasures in a nutshell. In the following, we assemble IPv6 vulnerabilities and evaluate appropriate countermeasures to provide a complete and comprehensive checklist for researchers, developers and administrators. Furthermore, we deduce major future research challenges, namely address assignment and structure, securing local network dis-


I wish sarcasm was
available as a font.
yourecards
someecards.com

WHAT IS NEW?

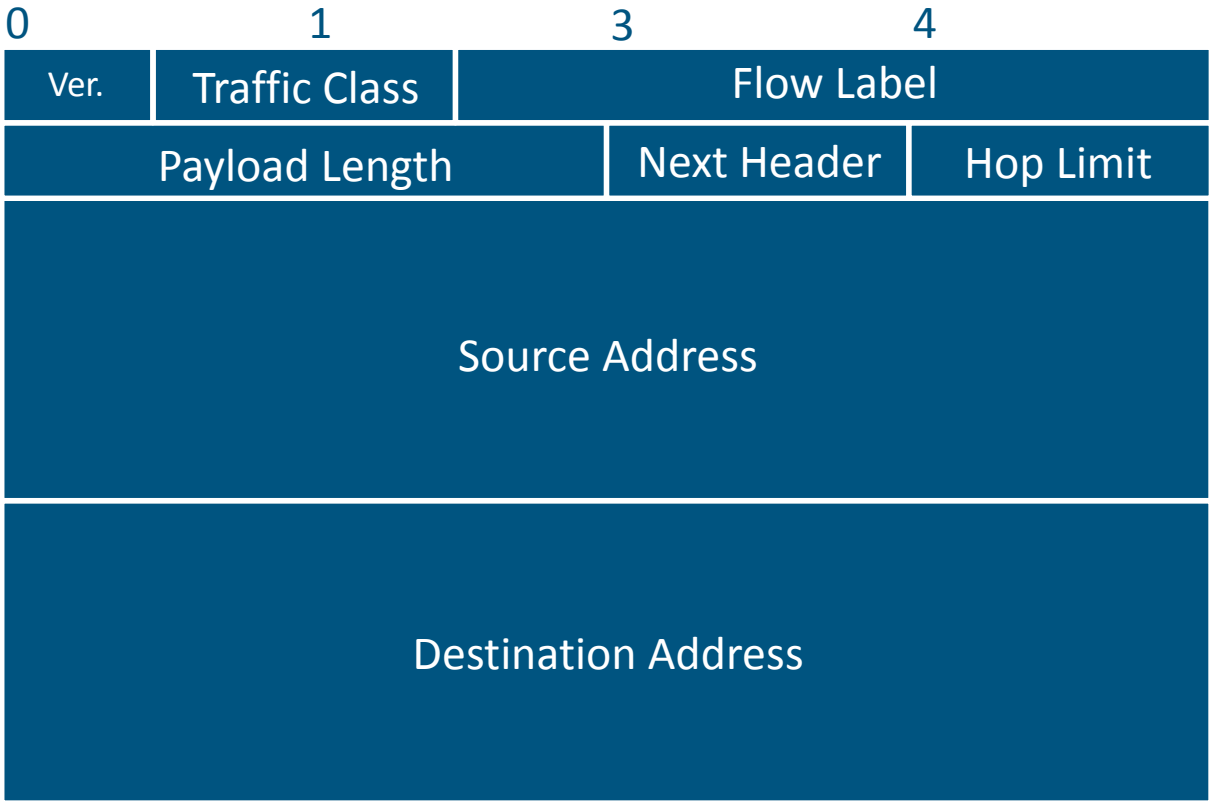
Remember the IPv4 Format …



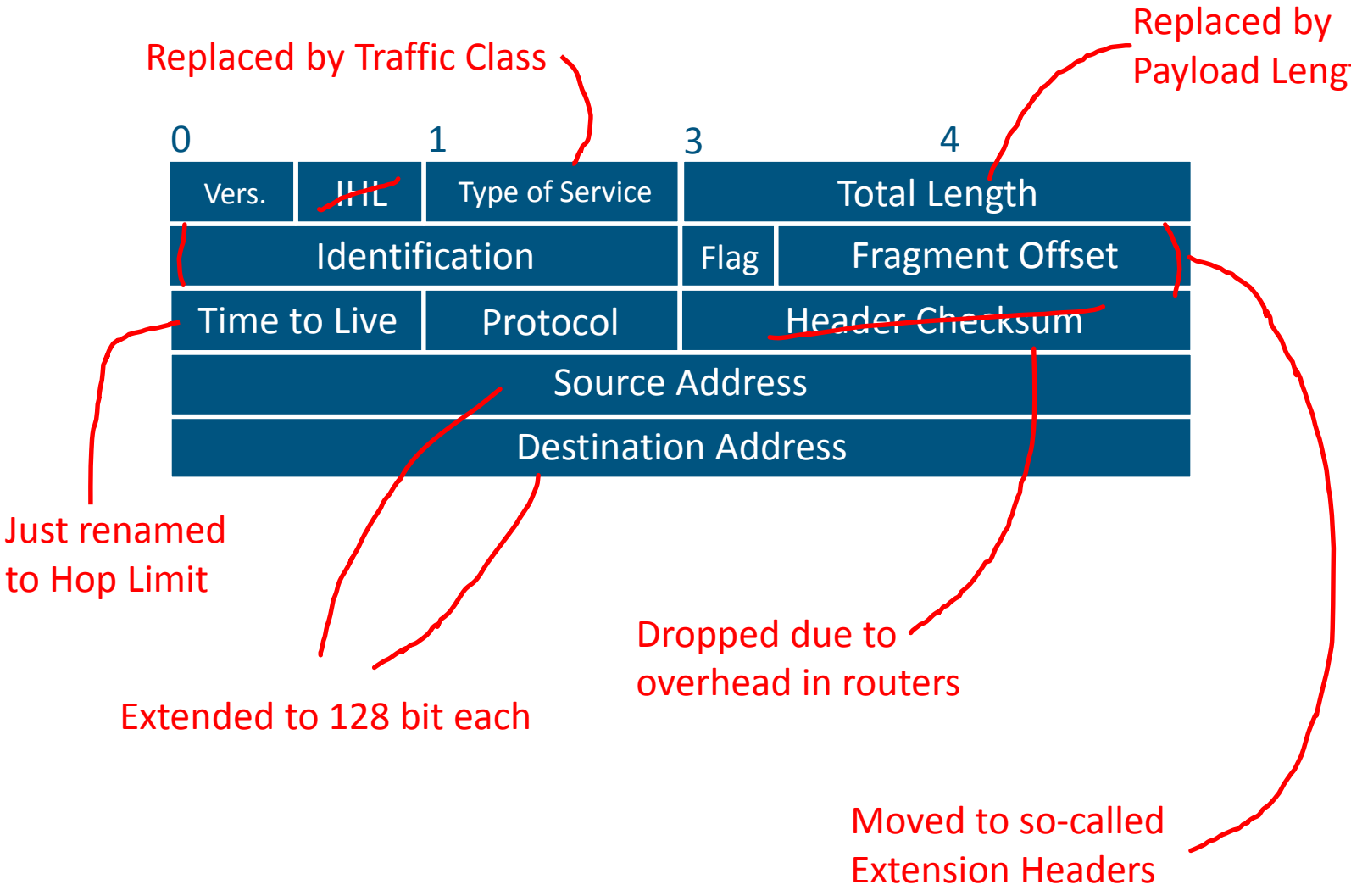
Variable header size

Minimal length of 20 byte

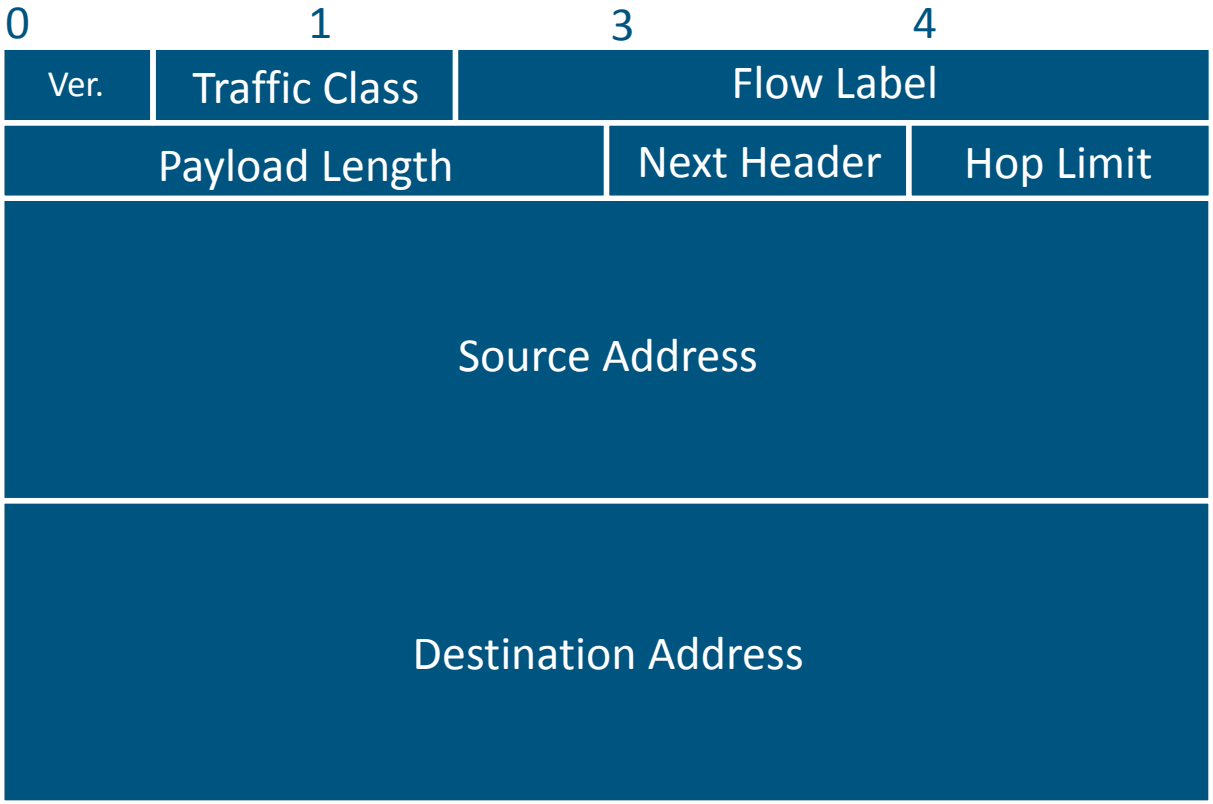
IPv6 Header Format



What happend to …?

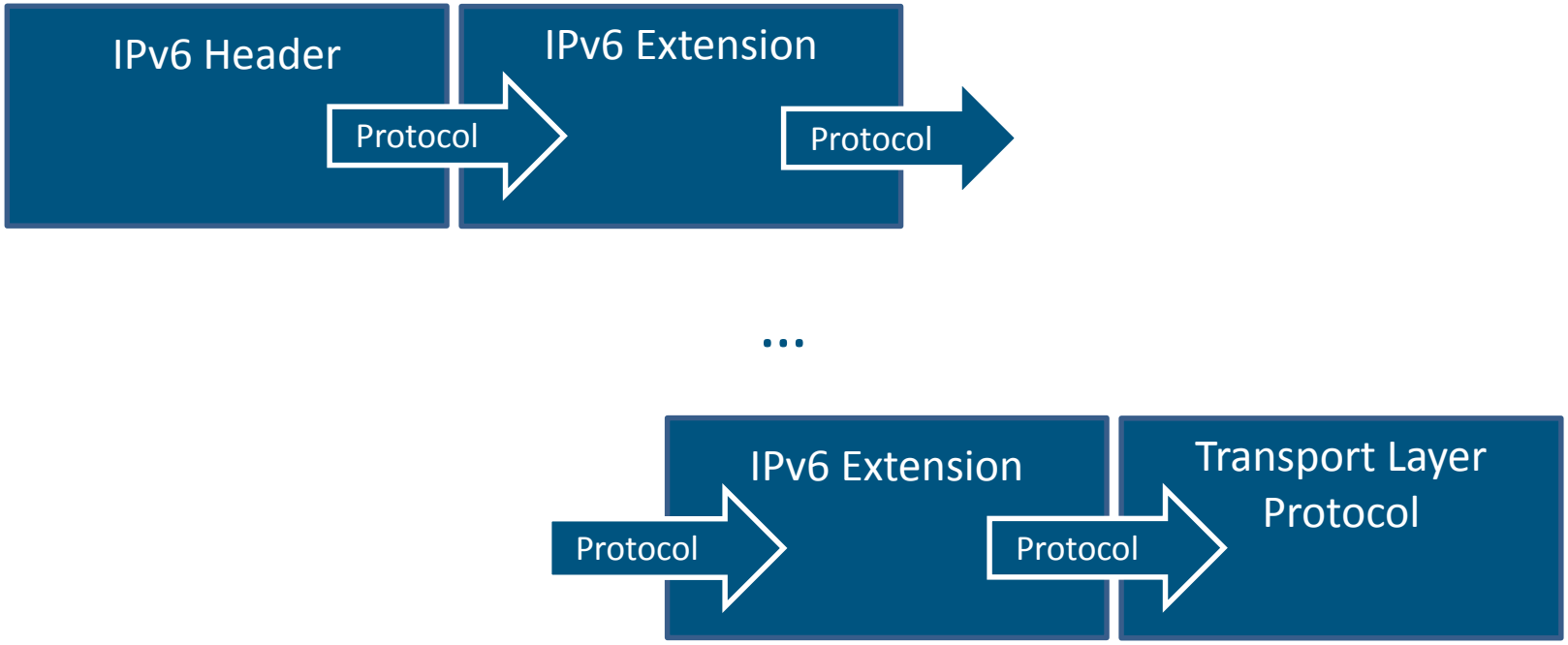


IPv6 Header Format



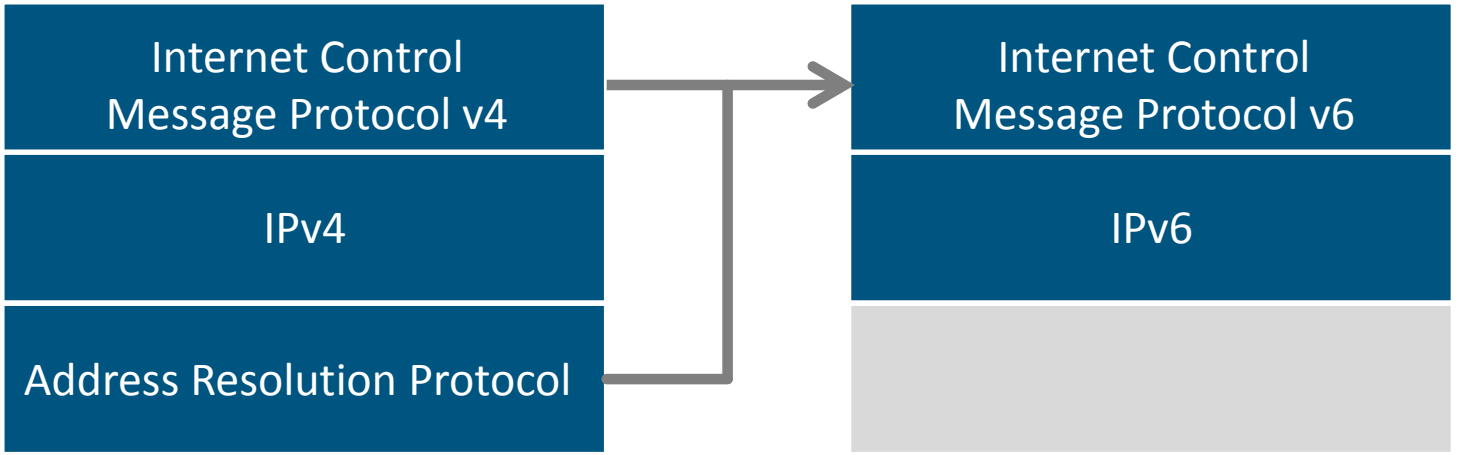
SECURITY VULNERABILITIES

Extension Headers



- Hop-by-Hop Options Header
- Routing Header
- Destination Options Header
- Fragment Header

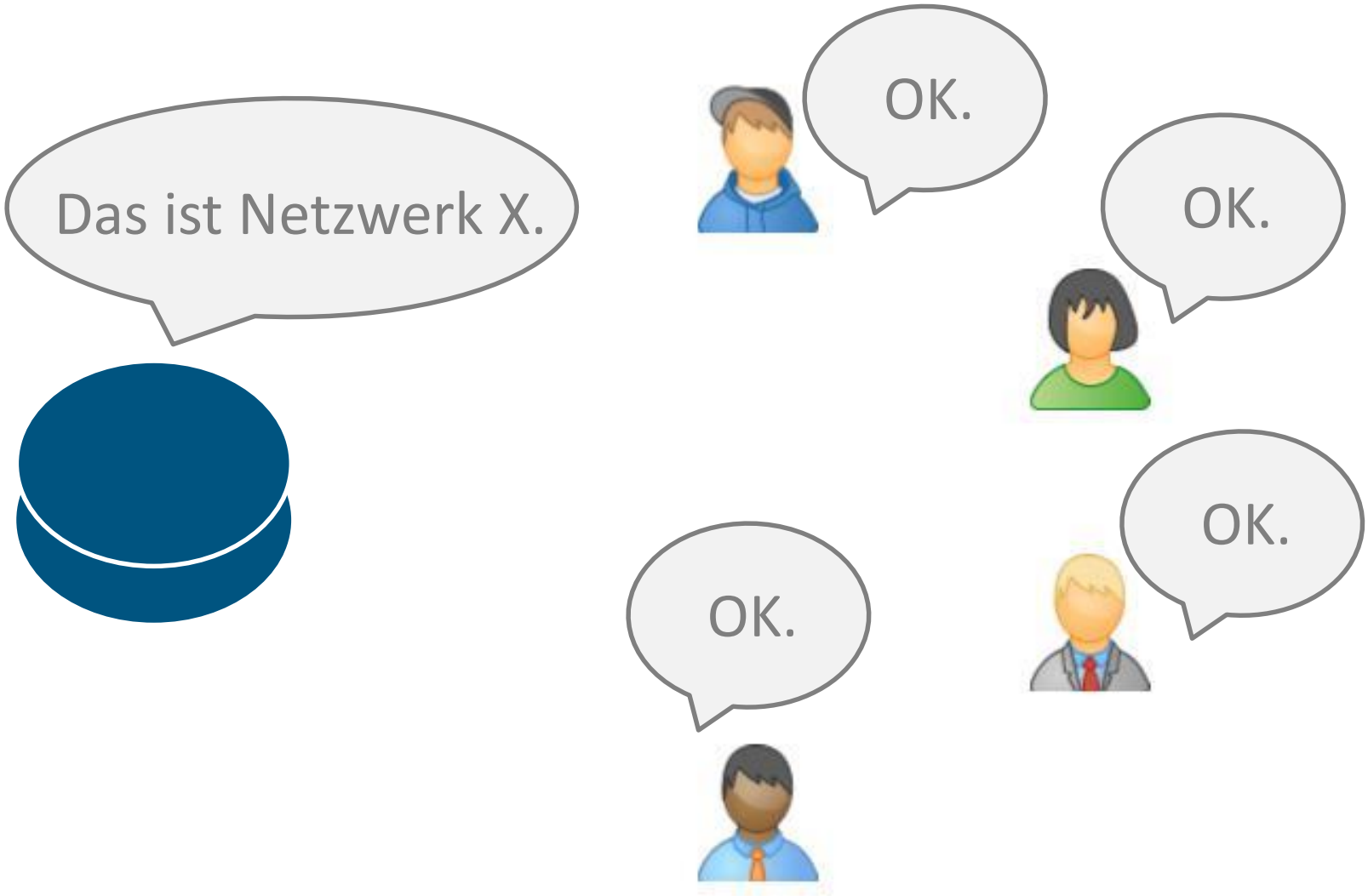
Internet Control Message Protocol



Don‘t block ICMPv6 totally!

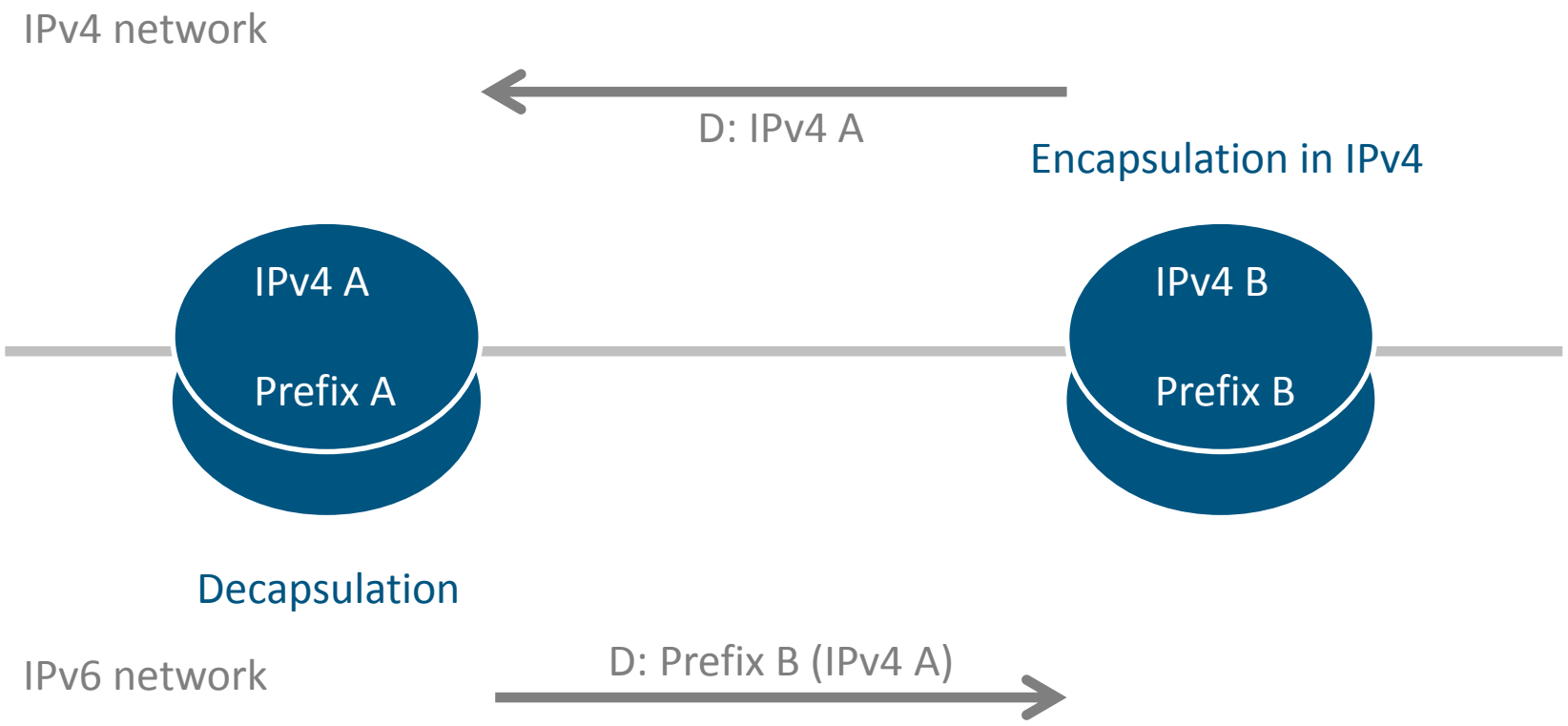
Router Advertisments

Router Advertisments

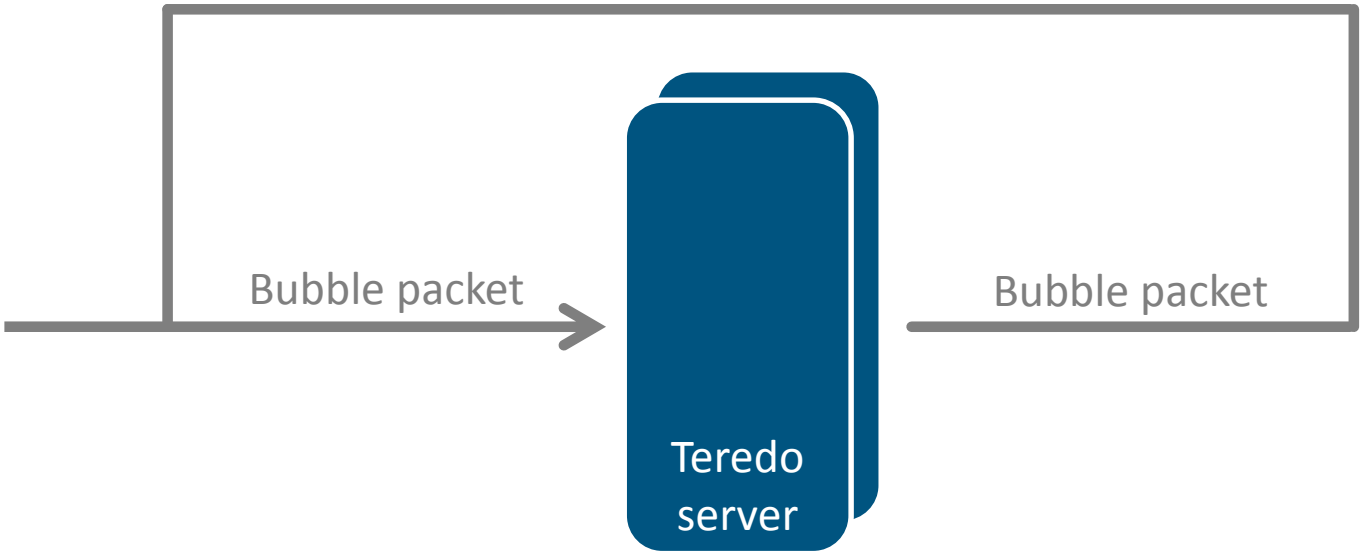


Router Advertisements

Routing Loops



Teredo Server Loop



Indefinite loop

Multicast Listener

… see next talk …

PRIVACY VULNERABILITIES

IPv6 Addresses

General Format

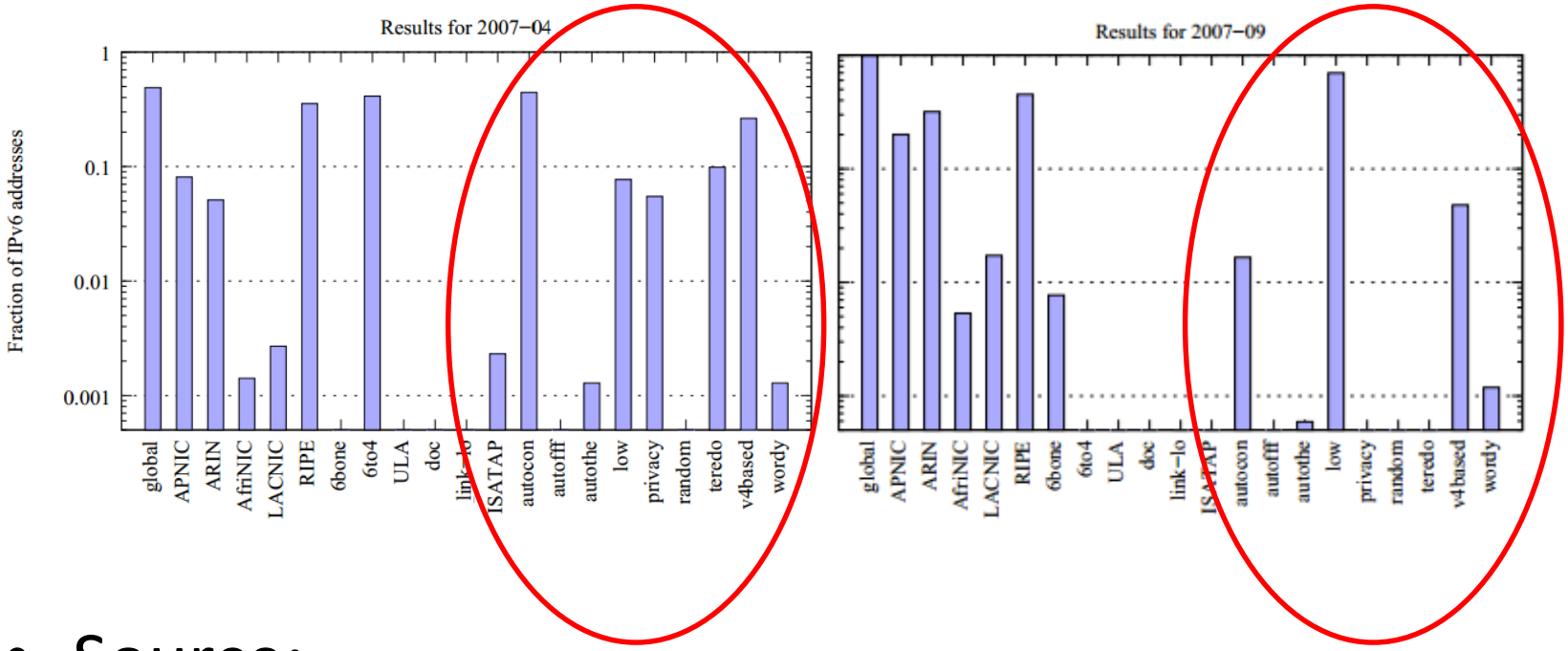
Interface Identifier

Modified EUI-Format, Privacy Extension, DHCP, Manually assigned, etc.

Reconaissance

End nodes

Routers



- Source:

  Malone D., „Observation of IPv6 Addresses“, 2008

Reconnaissance

18 446 744 073 709 551 616
Interface Identifier in one /64

Educated guess necessary:

DHCP range

Low numbers

NIC vendor

IPv4-based addresses

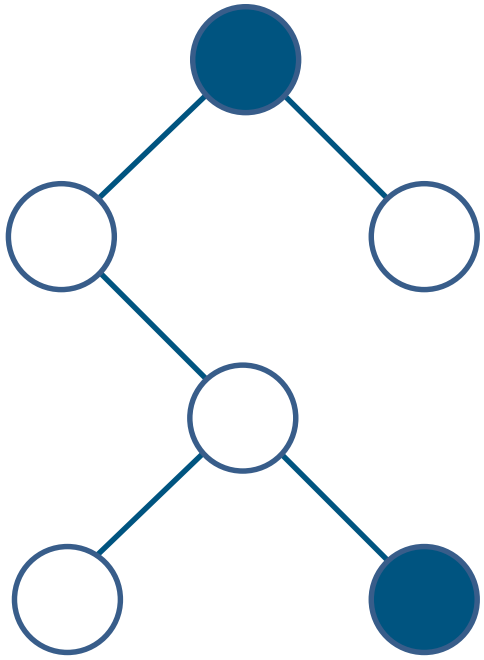
Multicast addresses

FF:FE from modified EU-64

DNS

Memorable pattern

Example:
Limit search by Reverse DNS



Reverse DNS:

[IPv6 address].ip6.arp

↓

NXDOMAIN

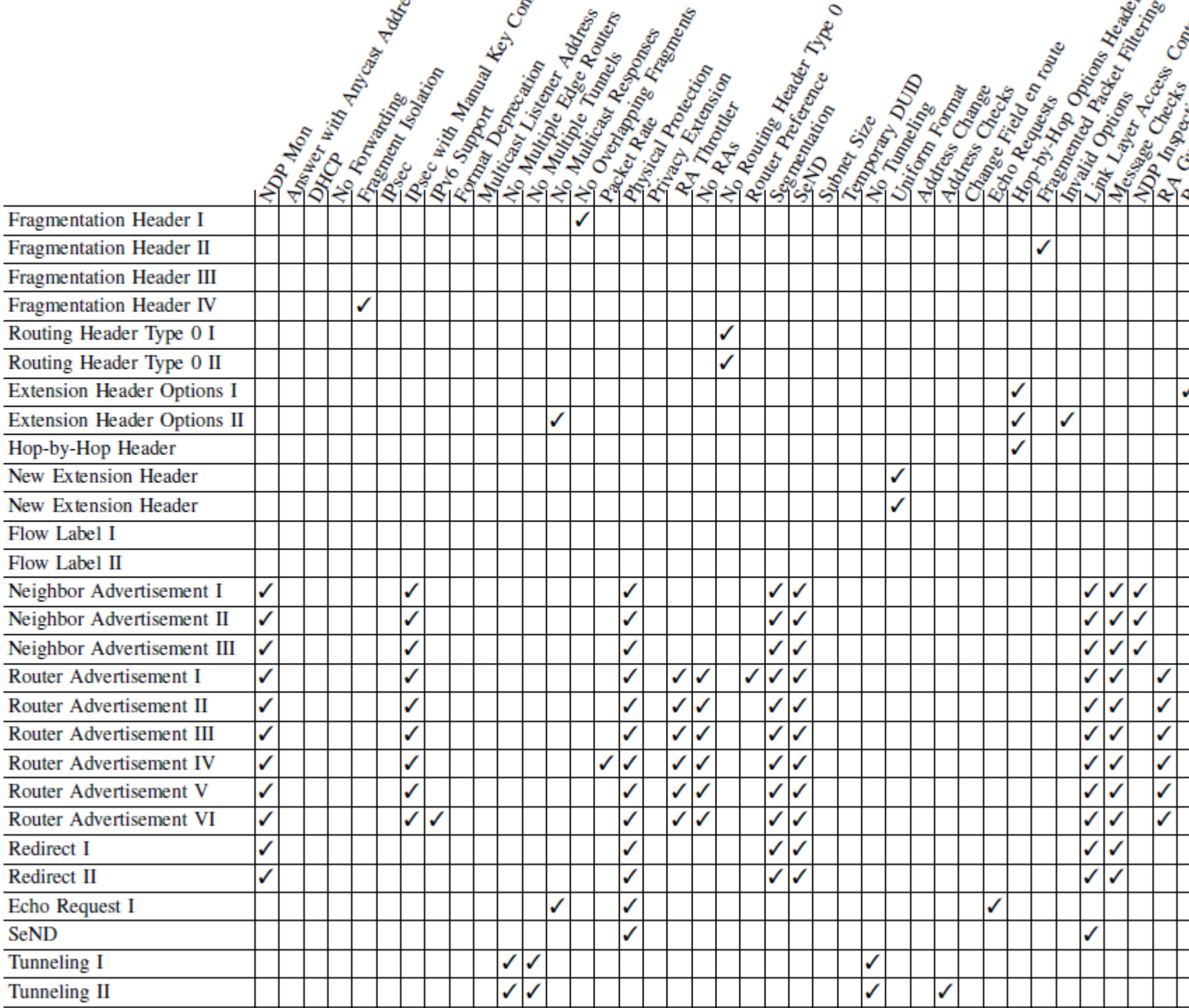
NOERROR

(empty non-terminals)

METHODOLOGY

	ID	Vulnerability	Action	Object	Target	Unauthorized Result	Orig
Security	v01	Fragmentation Header I	send	overlapping fragments		modified header fields	design
	v02	Fragmentation Header II	send	port number in second fragment		middlebox evasion	design
	v03	Fragmentation Header III	flood	fragments		memory shortage	design
	v04	Fragmentation Header IV	flood	atomic fragments		packet loss	design
	v05	Routing Header Type 0 I	send	routing header		traffic amplification	design
	v06	Routing Header Type 0 II	send	routing header		middlebox evasion	design
	v07	Extension Header Options I	send	router alert option		increased workload	design
	v08	Extension Header Options II	spoof	invalid 10xxxx option	multicast address	multiple responses	design
	v09	Hop-by-Hop Header	send	hop-by-hop header		increased workload	design
	v10	New Extension Header	send	unknown extension header		middlebox evasion	design
	v11	New Extension Header	send	unknown extension header		increased workload	design
	v12	Flow Label I	send	different flow labels		memory shortage	design
	v13	Flow Label II	send	existing flow label		quality-of-service theft	design
	v14	Neighbor Advertisement I	spoof	neighbor advertisement		wrongly resolved address	design
	v15	Neighbor Advertisement II	spoof	neighbor advertisement		traffic redirection	design
	v16	Neighbor Advertisement III	spoof	neighbor advertisement		address assignment prevention	design
	v17	Router Advertisement I	spoof	router advertisement		new default router	design
	v18	Router Advertisement II	spoof	router advertisement		removed default router	design
	v19	Router Advertisement III	spoof	router advertisement		wrong locally-announced prefix	design
	v20	Router Advertisement IV	flood	router advertisement		multiple address assignment	implemen
	v21	Router Advertisement V	spoof	router advertisement		prevention of DHCP assignment	design
	v22	Router Advertisement VI	send	router advertisement		IPv6 activation	implemen
	v23	Redirect I	spoof	redirect		redirected traffic	design
	v24	Redirect II	spoof	redirect		wrong locally-announced node	design
	v25	Echo Request I	spoof	echo request	multicast address	multiple responses	implemen
	v26	SeND	send	authenticated messages		increased workload	design
	v27	Tunneling I	send	IPv6 packet as IPv4 payload		middlebox evasion	implemen
	v28	Tunneling II	send	tunnel packet	relay router	cycling packet	implemen
	v29	Tunneling III	send	tunnel packet		cycling packet	configura
	v30	Teredo	send	Teredo bubble	server	cycling packet	design
	v31	Nesting	insert	packet into packet		packet overhead	configura
	v32	Fragmentation Header V	send	packet too big		inclusion of atomic fragments	design
	v33	Neighbor Discovery	scan		subnetwork	memory shortage	implemen
	v34	Forwarding	send	returning packet		traffic amplification	design

ID	Countermeasure	Action	Object
	Detective		
c01	NDP Mon	log	inconsistent NDP msg.
	Preventative		
c02	Use Anycast Address	respond	with anycast as source address
c03	DHCP	assign	addresses statefully
c04	No Forwarding	prohibit	forwarding over same interface
c05	Fragment Isolation	isolate	atomic from other fragments
c06	IPsec	encrypt	packets
c07	IPsec with Manual Keys	encrypt	packets
c08	No IPv6 Support	disable	IPv6
c09	Format Deprecation	prohibit	modified EUI format
c10	Multicast Listener Address	assign	lowest address to router
c11	No Multiple Edge Routers	disable	other edge routers
c12	No Multiple Tunnels	disable	other tunnels
c13	No Multicast Responses	prohibit	answers to multicast addresses
c14	No Overlapping Fragments	prohibit	overlapping fragments
c15	Packet Rate	limit	packet rate
c16	Physical Protection	prohibit	physical access to network
c17	Privacy Extension	assign	temporary random address
c18	RA Throttler	limit	router advertisements
c19	No RAs	disable	router advertisements
c20	No Routing Header Type 0	prohibit	routing header type 0
c21	Router Preference	assign	highest preference
c22	Segmentation	segment	network
c23	SeND	encrypt	NDP messages
c24	Subnet Size	minimize	subnet size
c25	Temporary DUID	assign	temporary DUID
c26	No Tunneling	disable	all tunnels
c27	Uniform Format	limit	number of ext. header formats
	Reactive		
c28	Address Change	assign	new addresses simultaneously
c29	Address Checks	filter	inconsistent addresses
c30	Change Field en route	assign	default value
c31	Echo Requests	filter	echo requests
c32	Hop-by-Hop Options	filter	hop-by-hop extension header
c33	Routing Header	filter	routing headers



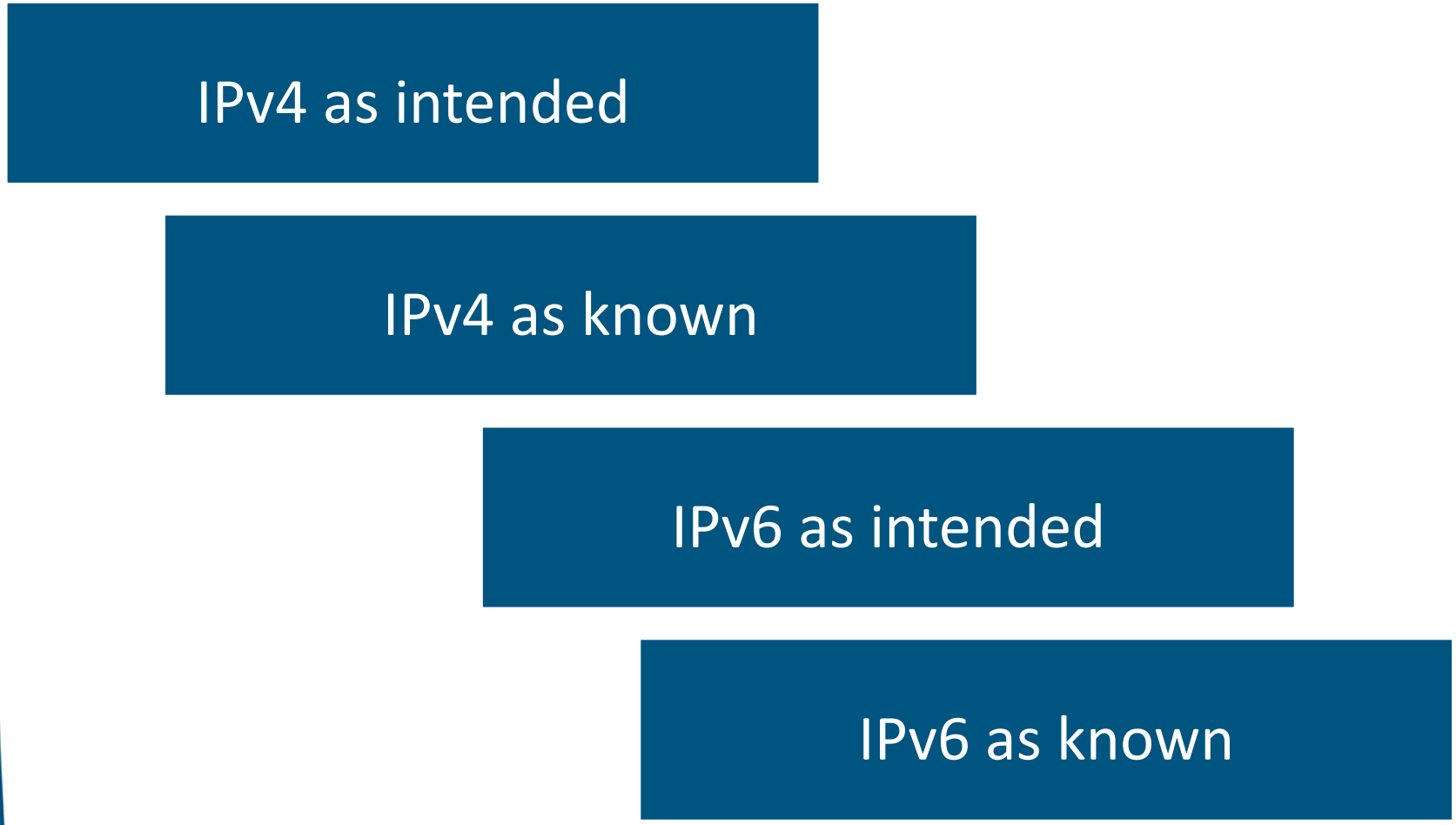
Future Challenges

Addressing

Securing the Local Network

Reconnaissance

Generation Next – Generation Best?



Thank you!

Johanna Ullrich
SBA Research
jullrich@sba-research.org