Firewall Security Assessment and Benchmarking
IPv6 Firewall Load Tests

Eldad Zack, European Advanced Networking Test Center

zack@eantc.de

June 30th, 2013

IPv6 Hackers Meeting in Berlin: www.ipv6hackers.org

EANTC

EUROPEAN ADVANCED NETWORKING TEST CENTER

Agenda

- Test Suite
- Expectations
- Tested devices
- Results

About the
European Advanced Networking Test Center

- Vendor independent network quality assurance since 1991
- Unique technical expertise of network design and testing in latest technology areas
- 20-year testing experience matches highest quality standards

Tested by EANTC 2013

Business Areas

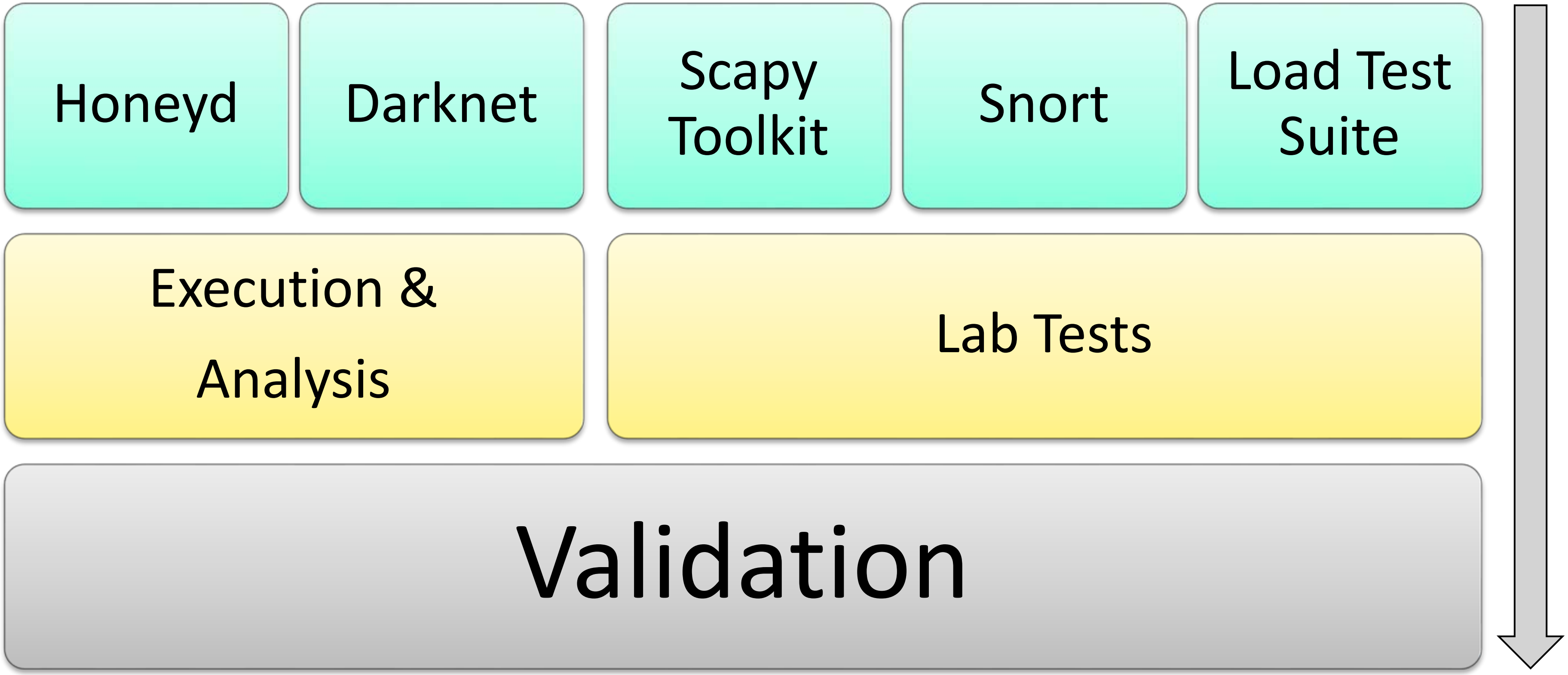
- Test and certification of network components for manufacturers
- Network design consultancy and proof of concept testing for service providers
- Request for Proposal (RfP) support, acceptance testing and network audits for large enterprises and government organizations
- Vendor neutral technology seminars

EANTC Berlin, Germany

IPv6 Intrusion Detection Research Project

- Partners:
  - University of Potsdam (Universität Potsdam)
  - Beuth University of Applied Sciences (Beuth-Hochschule für Technik Berlin)
  - EANTC AG
- Associate Partner:
  - STRATO AG
- Sponsered by the Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung).
- Project time frame: 2011-2013

Workplan



Honeyd

Darknet

Scapy Toolkit

Snort

Load Test Suite

Execution & Analysis

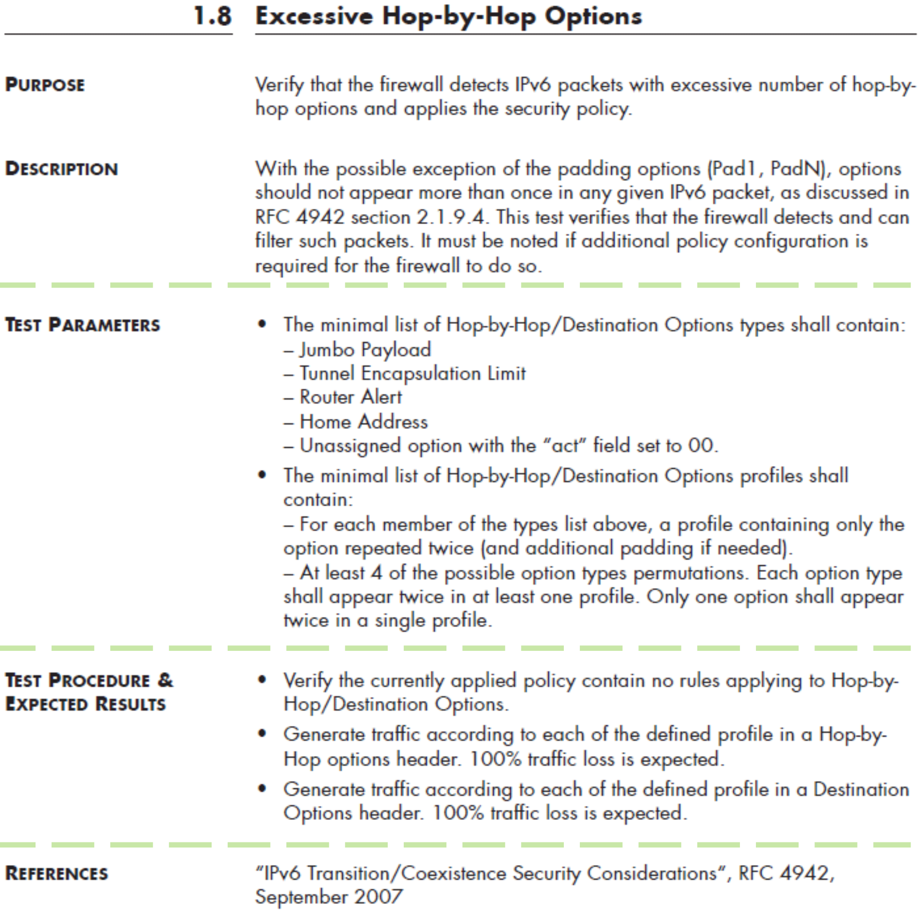
Lab Tests

Validation

www.idsv6.de

Test Case Structure

- Exposition
- Attributes
- Execution
- References



1.8 Excessive Hop-by-Hop Options

Purpose

Verify that the firewall detects IPv6 packets with excessive number of hop-by-hop options and applies the security policy.

Description

With the possible exception of the padding options (Pad1, PadN), options should not appear more than once in any given IPv6 packet, as discussed in RFC 4942 section 2.1.9.4. This test verifies that the firewall detects and can filter such packets. It must be noted if additional policy configuration is required for the firewall to do so.

Test Parameters

- The minimal list of Hop-by-Hop/Destination Options types shall contain:
  – Jumbo Payload
  – Tunnel Encapsulation Limit
  – Router Alert
  – Home Address
  – Unassigned option with the "act" field set to 00.
- The minimal list of Hop-by-Hop/Destination Options profiles shall contain:
  – For each member of the types list above, a profile containing only the option repeated twice (and additional padding if needed).
  – At least 4 of the possible option types permutations. Each option type shall appear twice in at least one profile. Only one option shall appear twice in a single profile.

Test Procedure & Expected Results

- Verify the currently applied policy contain no rules applying to Hop-by-Hop/Destination Options.
- Generate traffic according to each of the defined profile in a Hop-by-Hop options header. 100% traffic loss is expected.
- Generate traffic according to each of the defined profile in a Destination Options header. 100% traffic loss is expected.

References

"IPv6 Transition/Coexistence Security Considerations", RFC 4942, September 2007

Test Suite

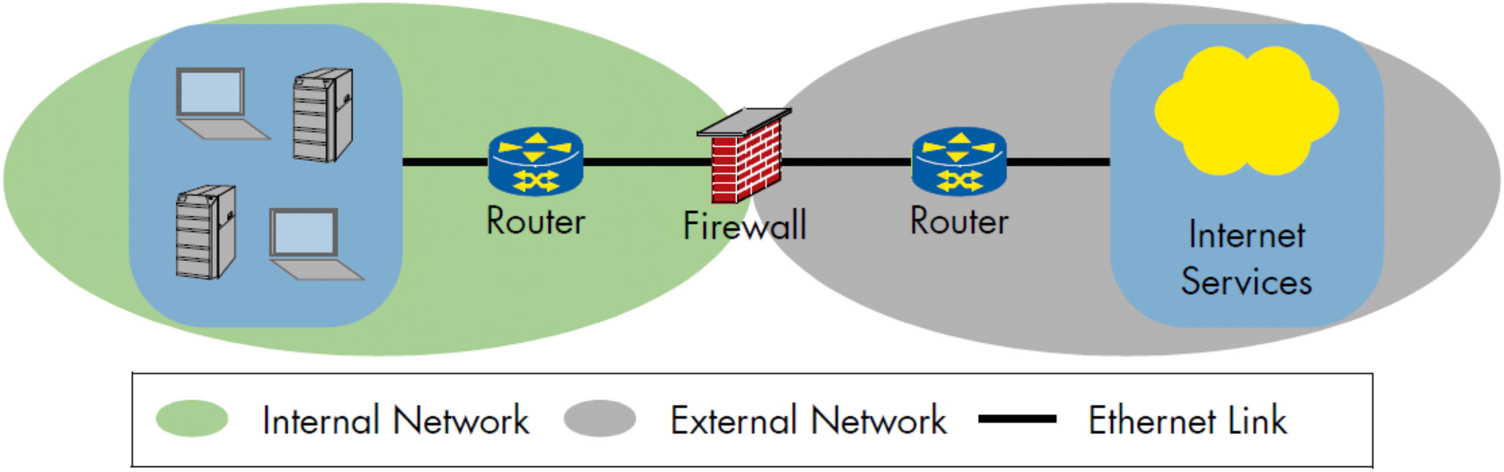
- 28 Test Cases
  - 11 Firewall Protocol Tests
  - 11 Firewall Load Tests
  - 6 IDS Tests
- Published under a Creative Commons license:

  http://www.idsv6.de/en/material.html

Firewall Load Tests
Test Setup

- Filters based on IETF RFCs 2544 and 5180
  25 IPv4 “drop” rules
  25 IPv6 “drop” rules

- Router



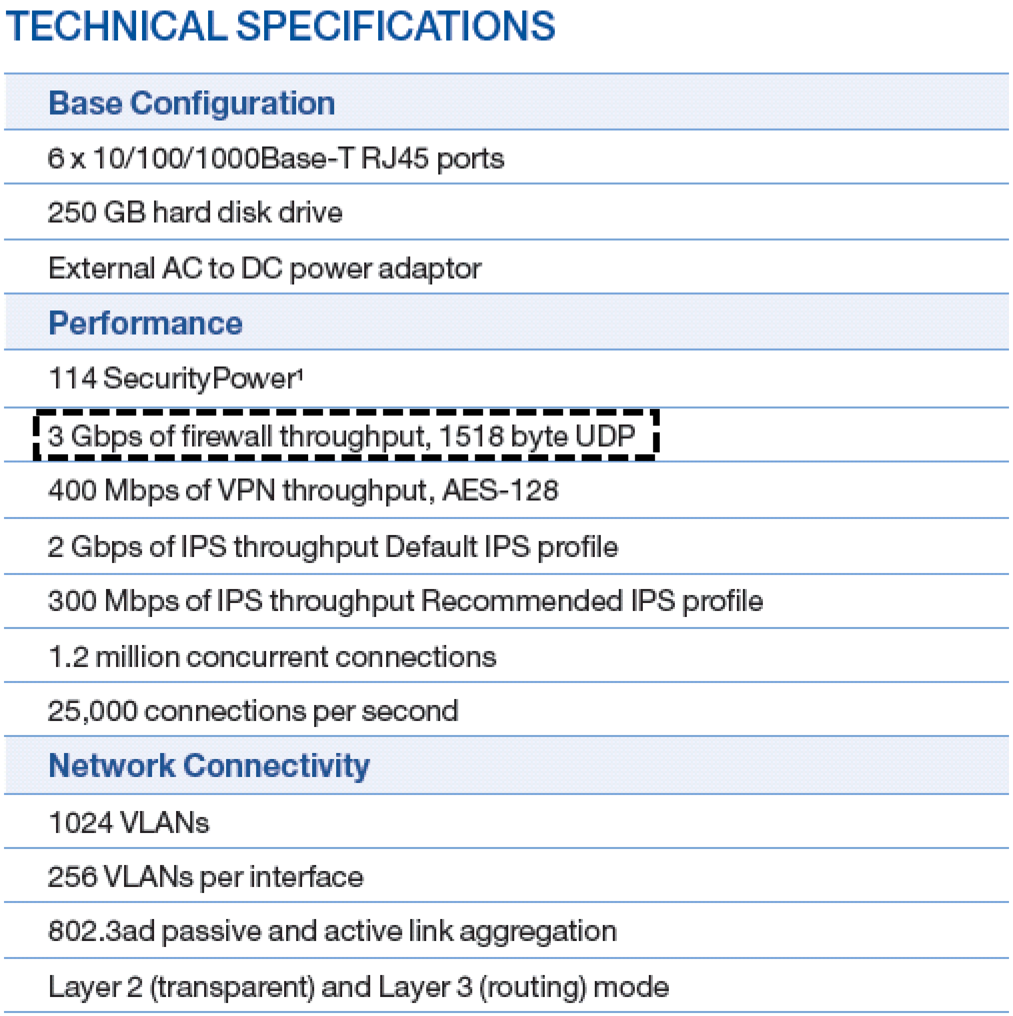
Device Under Test (#1)

Checkpoint Firewall

CP2210

Software Version

R75.10



TECHNICAL SPECIFICATIONS

Base Configuration
6 x 10/100/1000Base-T RJ45 ports
250 GB hard disk drive
External AC to DC power adaptor
Performance
114 SecurityPower[1]
3 Gbps of firewall throughput, 1518 byte UDP
400 Mbps of VPN throughput, AES-128
2 Gbps of IPS throughput Default IPS profile
300 Mbps of IPS throughput Recommended IPS profile
1.2 million concurrent connections
25,000 connections per second
Network Connectivity
1024 VLANs
256 VLANs per interface
802.3ad passive and active link aggregation
Layer 2 (transparent) and Layer 3 (routing) mode

Device Under Test (#2)

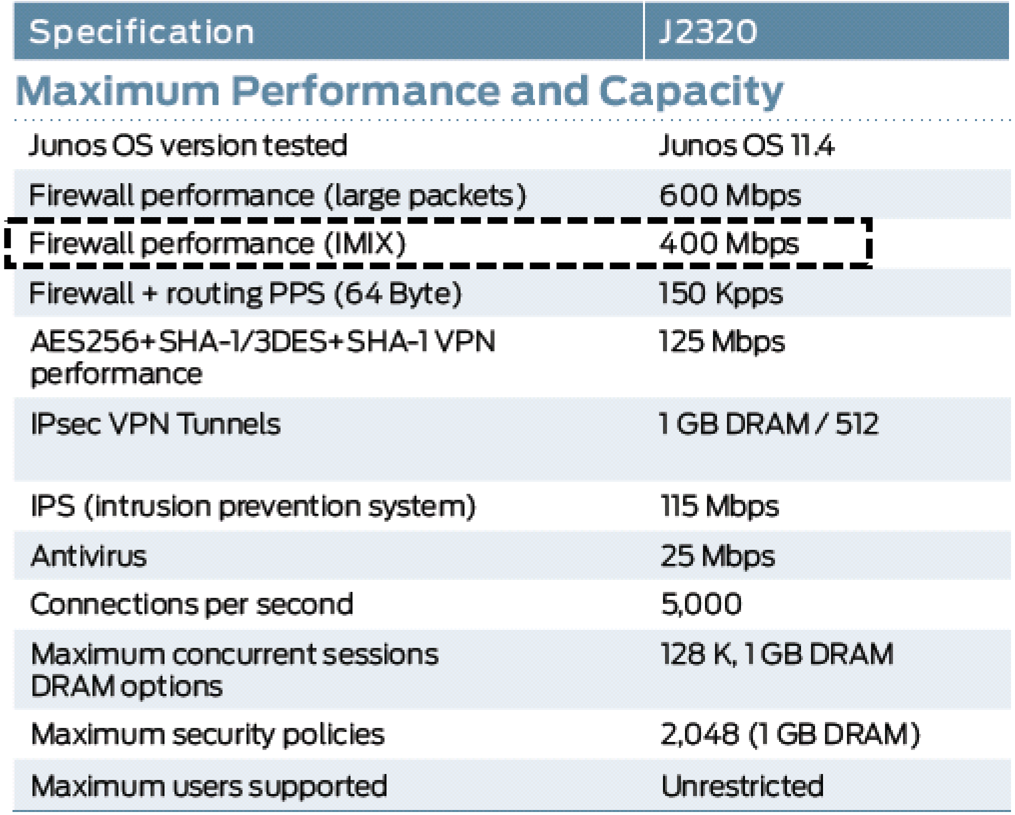
Juniper J2320

Service Router

(1GB DRAM Model)

Software Version

10.2R3.10



Specification	J2320
Maximum Performance and Capacity	
Junos OS version tested	Junos OS 11.4
Firewall performance (large packets)	600 Mbps
Firewall performance (IMIX)	400 Mbps
Firewall + routing PPS (64 Byte)	150 Kpps
AES256+SHA-1/3DES+SHA-1 VPN performance	125 Mbps
IPsec VPN Tunnels	1 GB DRAM / 512
IPS (intrusion prevention system)	115 Mbps
Antivirus	25 Mbps
Connections per second	5,000
Maximum concurrent sessions DRAM options	128 K, 1 GB DRAM
Maximum security policies	2,048 (1 GB DRAM)
Maximum users supported	Unrestricted

Layer 3 Performance Test
Prestaging: 100% IPv4

- Establish baseline

  Maximal, loss-free Layer 3 throughput

- IMIX (Internet Mix)

  Based on packet sizes from RFC 5180

Size (Bytes)	Weight
130	2
256	1
512	1
1024	1
1280	1
1518	1
Average:	**674.3 Bytes**

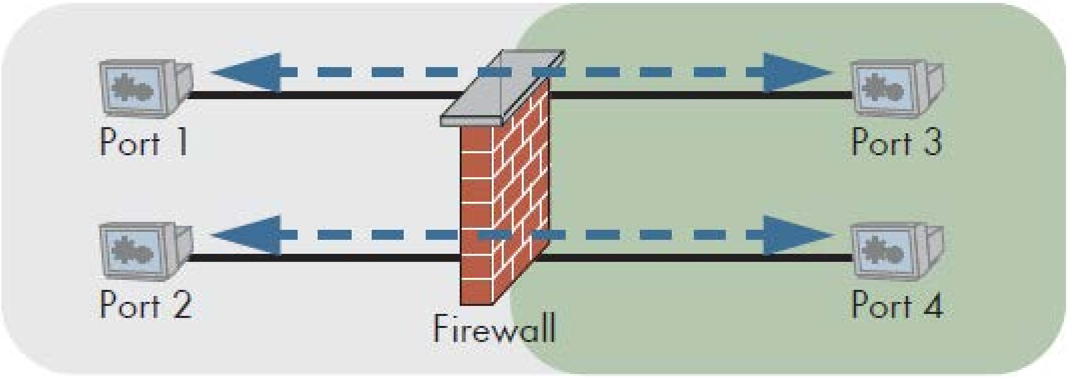
Prestaging: Checkpoint CP2210
Measurements According to Vendor Specifications (1/2)

- 5 Ports + 1 Management-Port

  4 used

- Vendor specifications: 3 Gbit/s with UDP, 1518 Bytes.

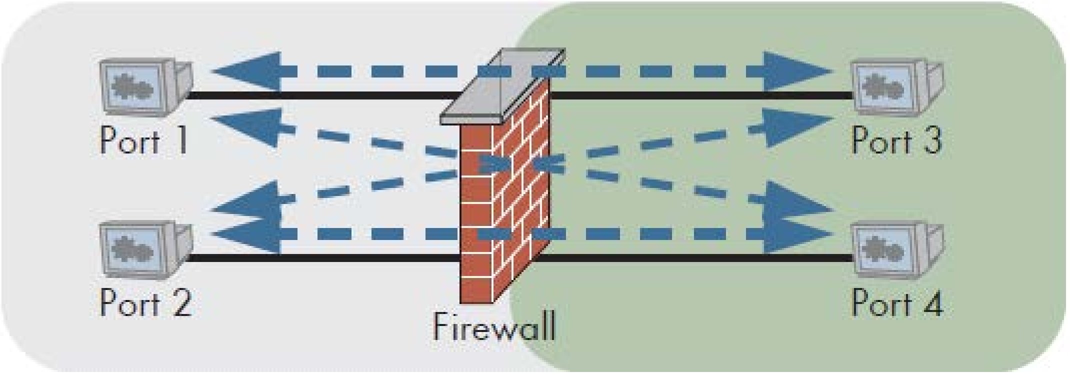
  EANTC Result (portwise):
  3 Gbit/s with UDP, 1518 Bytes



Prestaging: Checkpoint CP2210
Measurements According to Vendor Specifications (2/2)

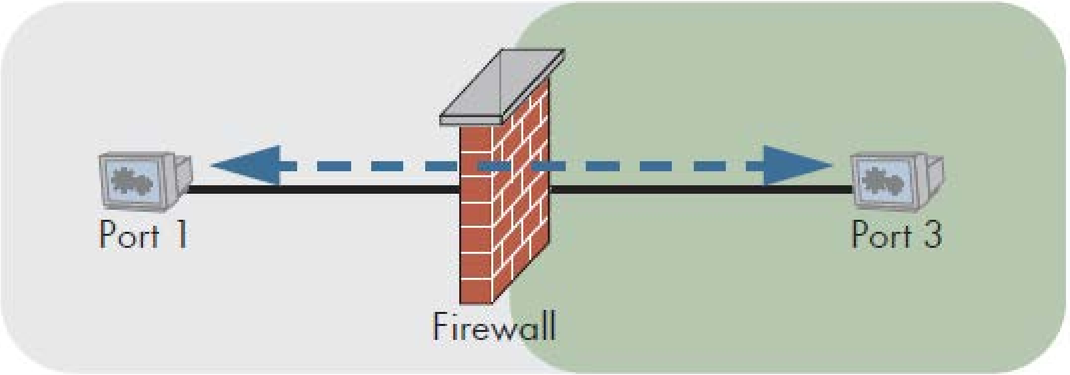
- Partial-Meshing (UDP, 1518 Bytes)
  EANTC Result:**2.7 Gbit/s.**

- With IMIX (instead of 1518 Bytes):
  EANTC Result:**1.3 Gbit/s.**

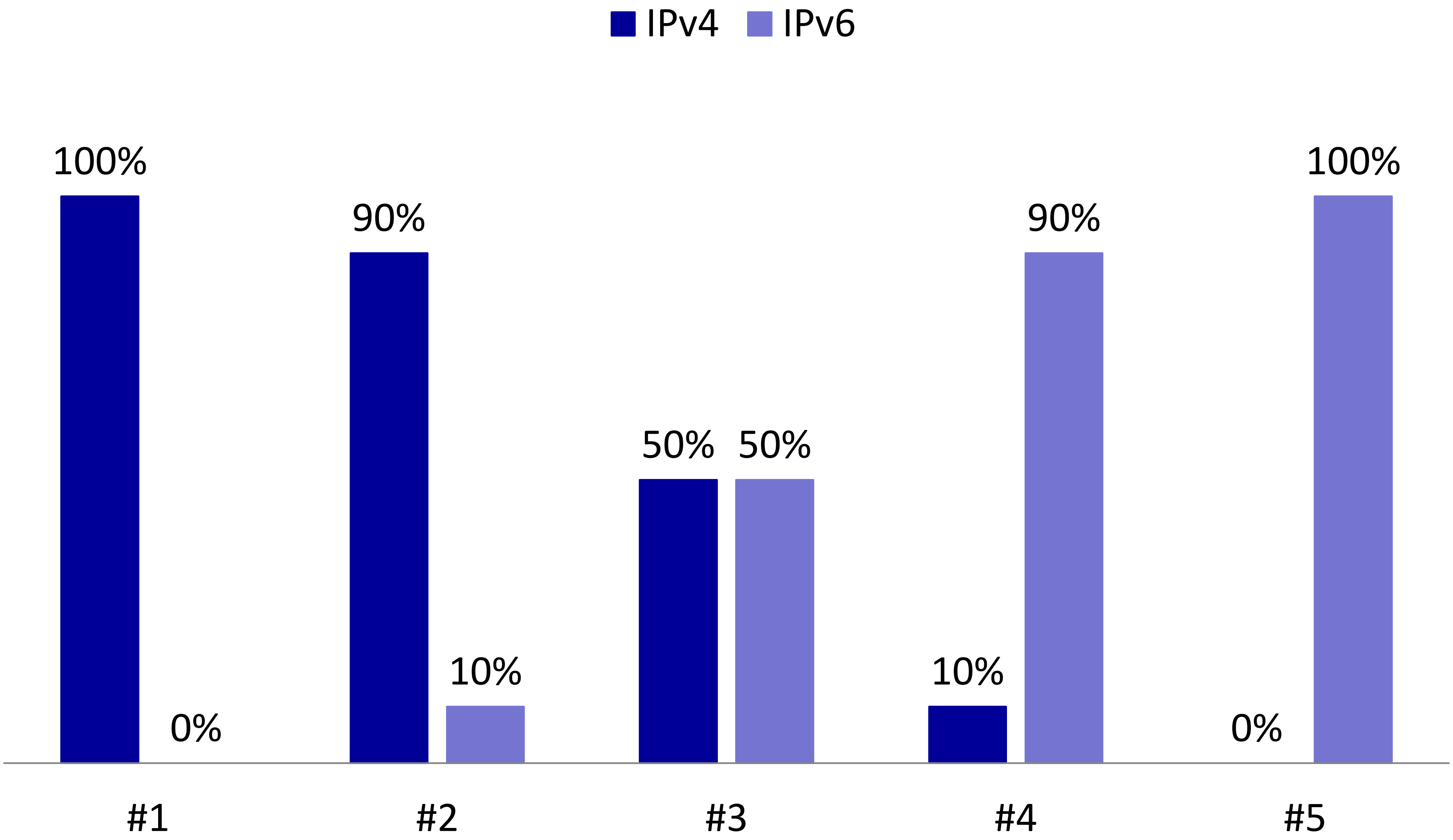


Prestaging: Juniper J2320
Measurements According to Vendor Specifications

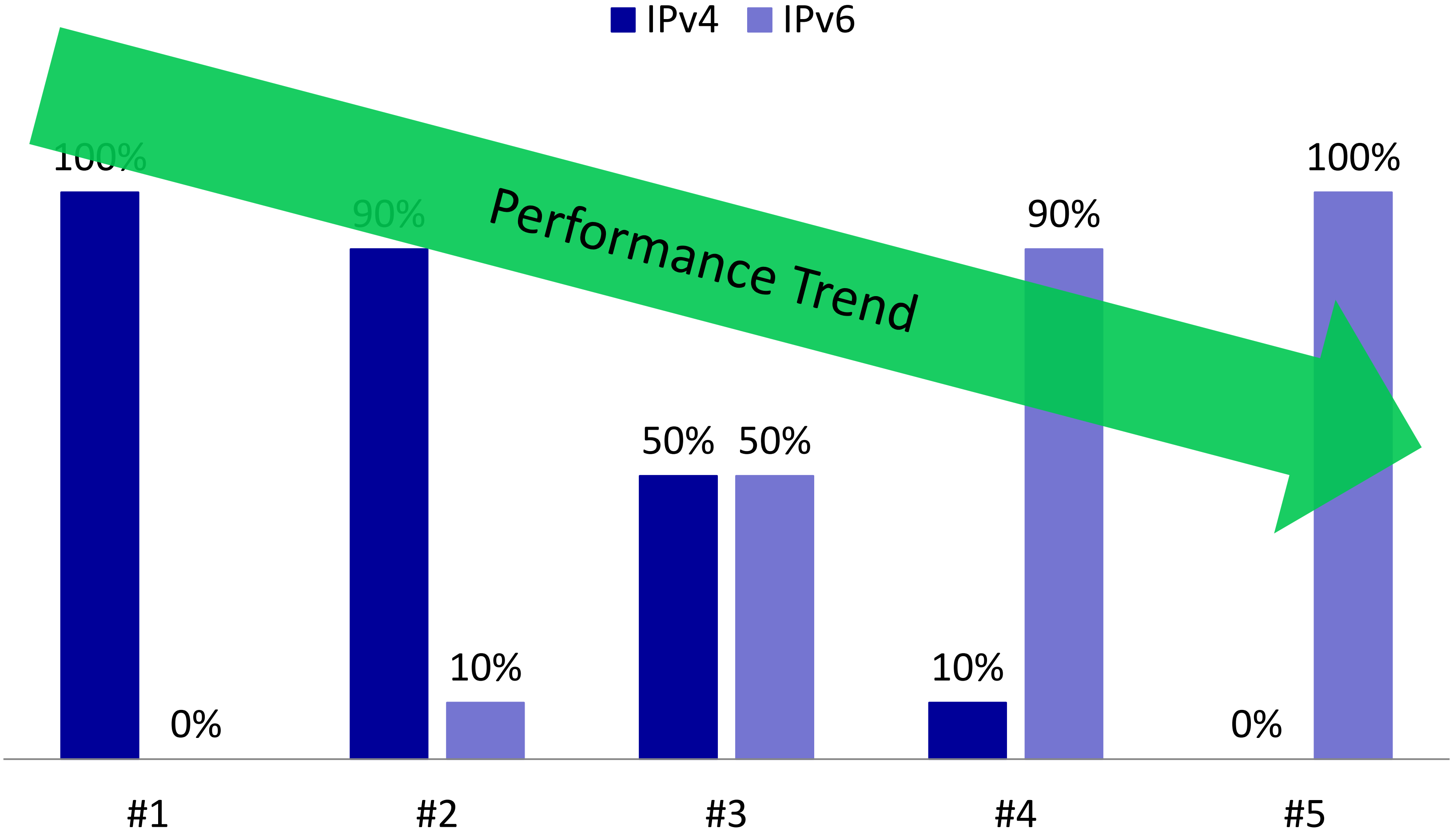
- 3 Ports + 1 Management-Port
  - 2 used
- Vendor Specifications:
  - 600 Mbit/s for “Large Packets”
  - 400 Mbit with IMIX
- EANTC Result:
  - 640 Mbit/s (with **IMIX**)



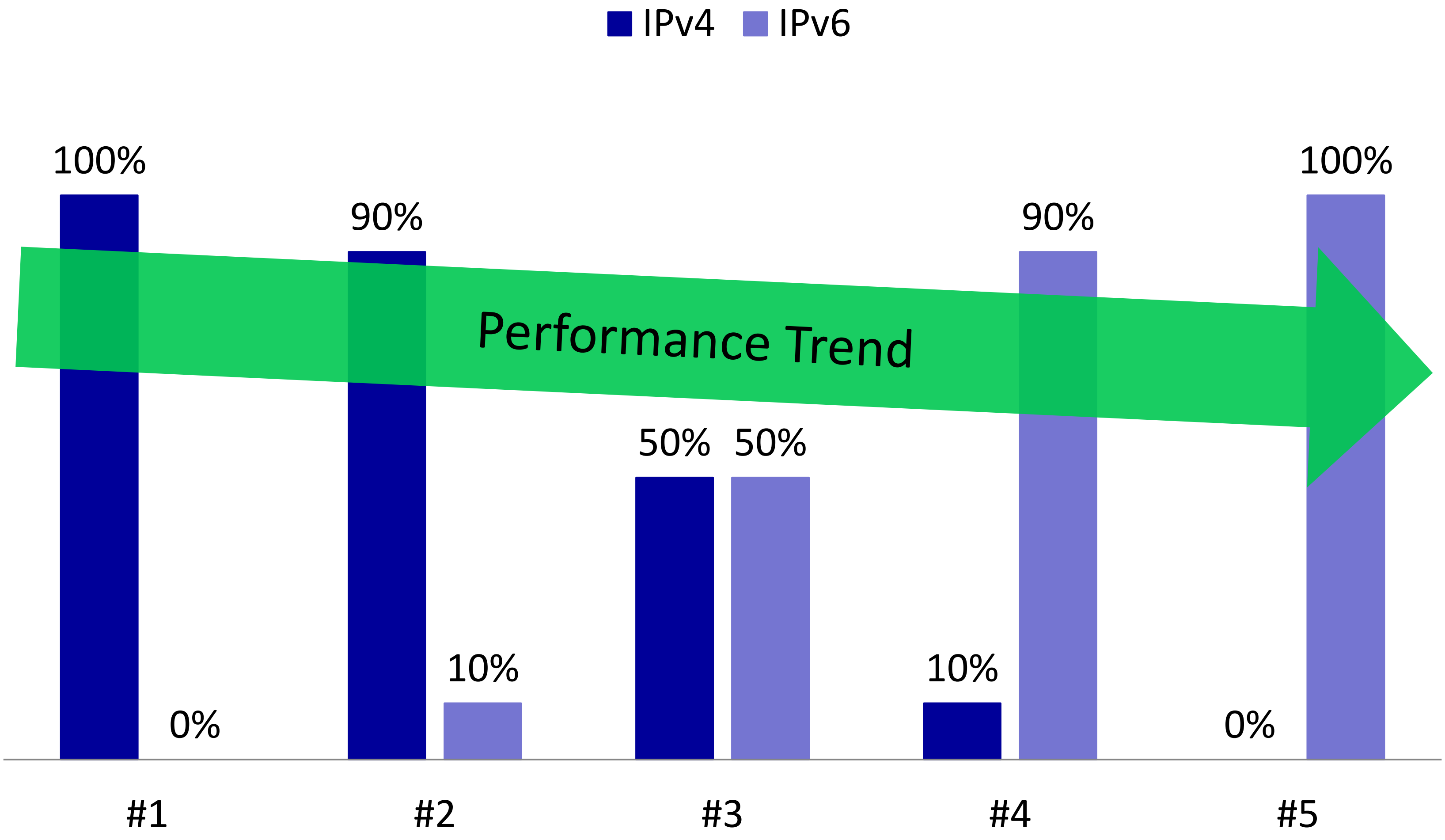
Coexistence Traffic Ratios (Based on RFC 5180) Expectations



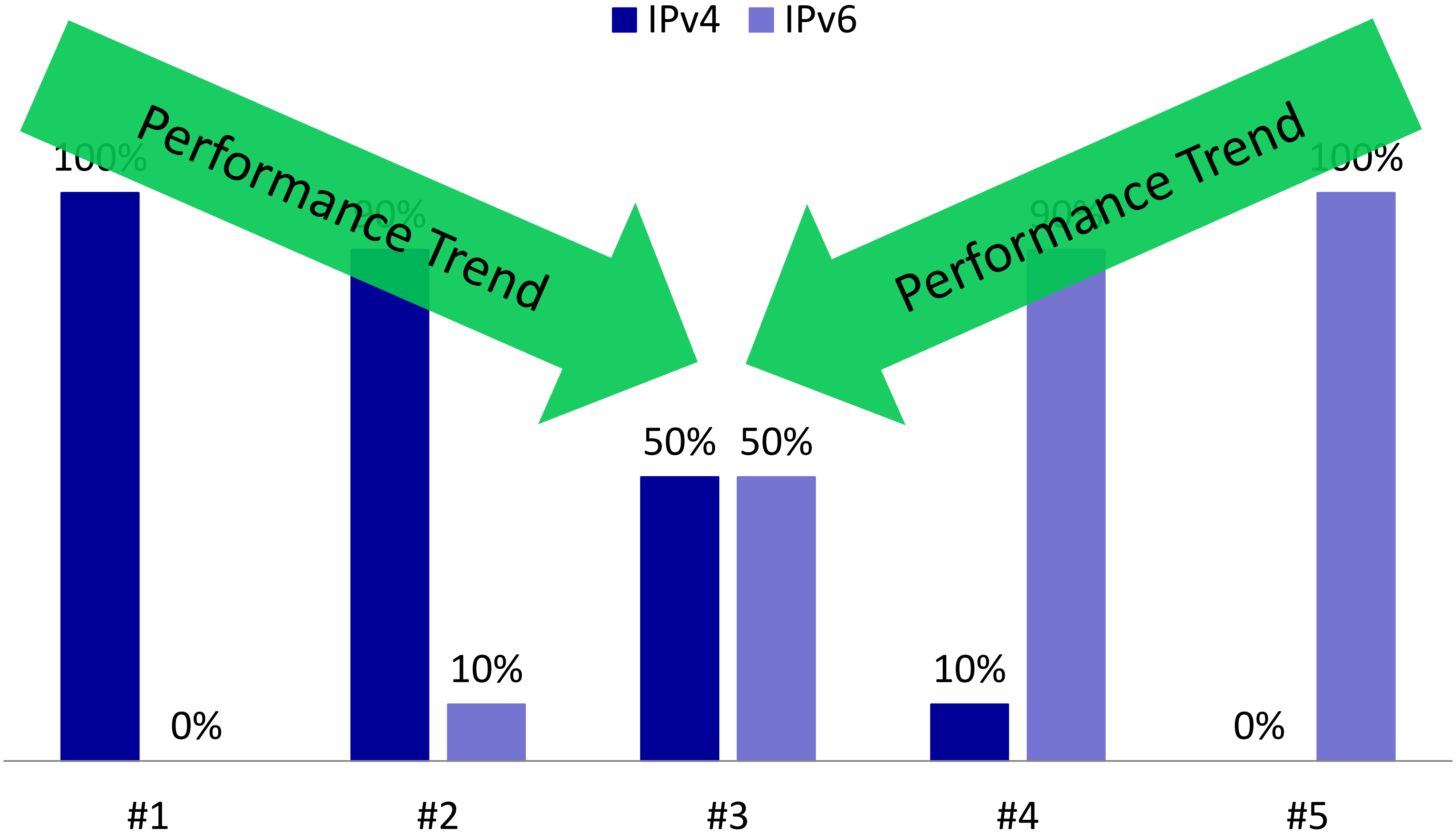
Coexistence Traffic Ratios
Strong Influence of IPv6 Traffic



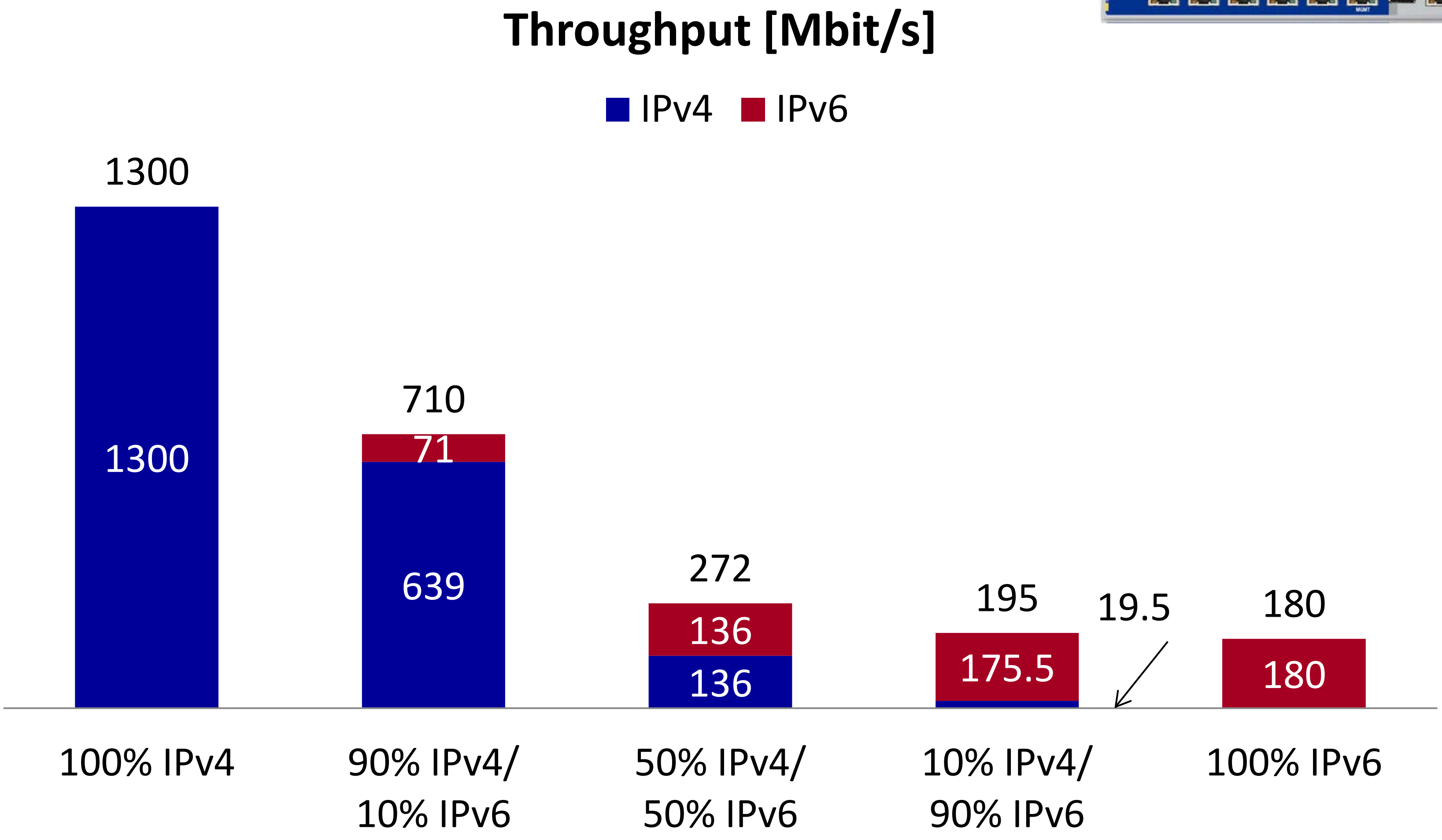
Coexistence Traffic Ratios
Light Influence of IPv6 Traffic



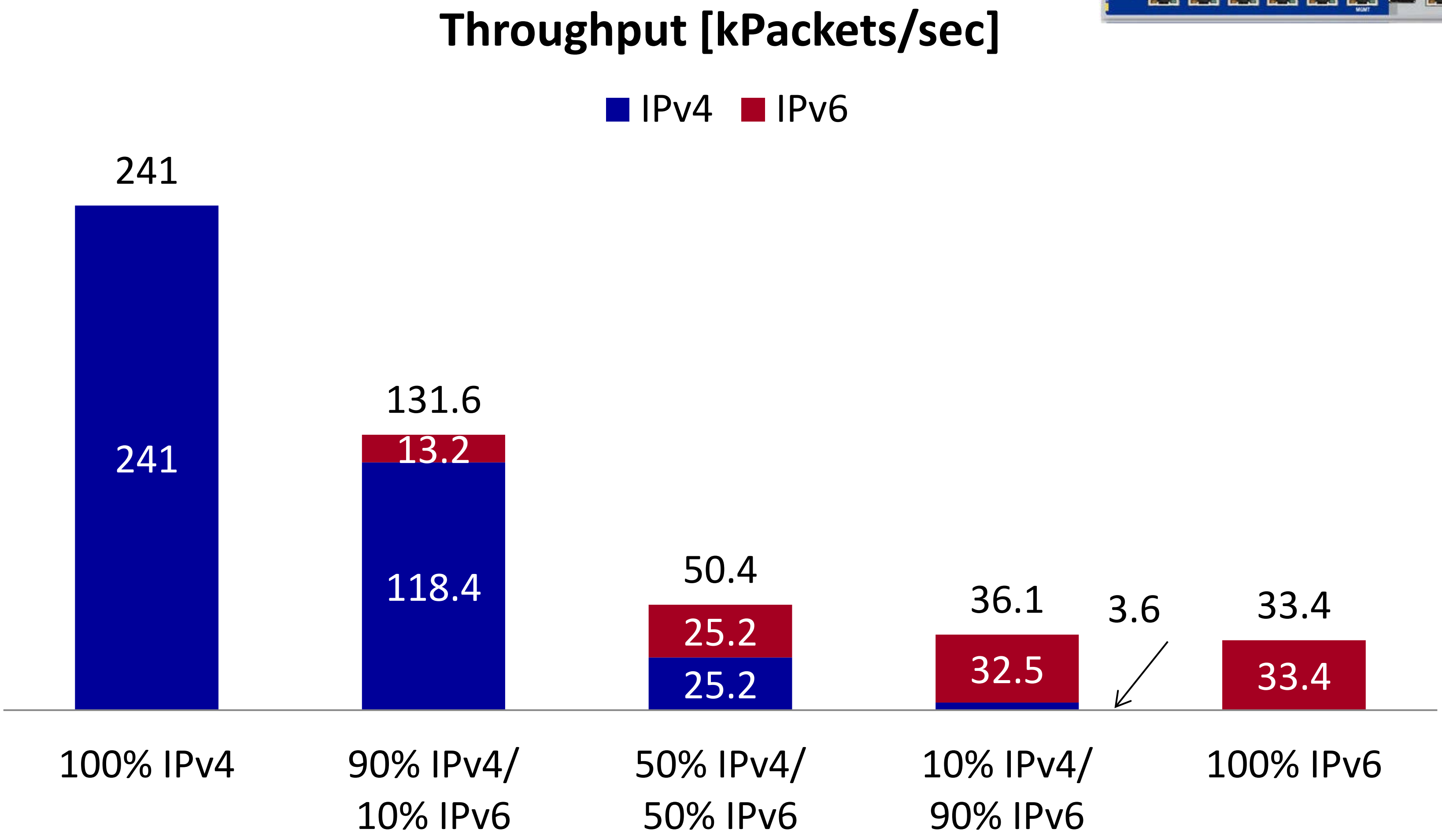
Coexistence Traffic Ratios
Dual-Stack Influence



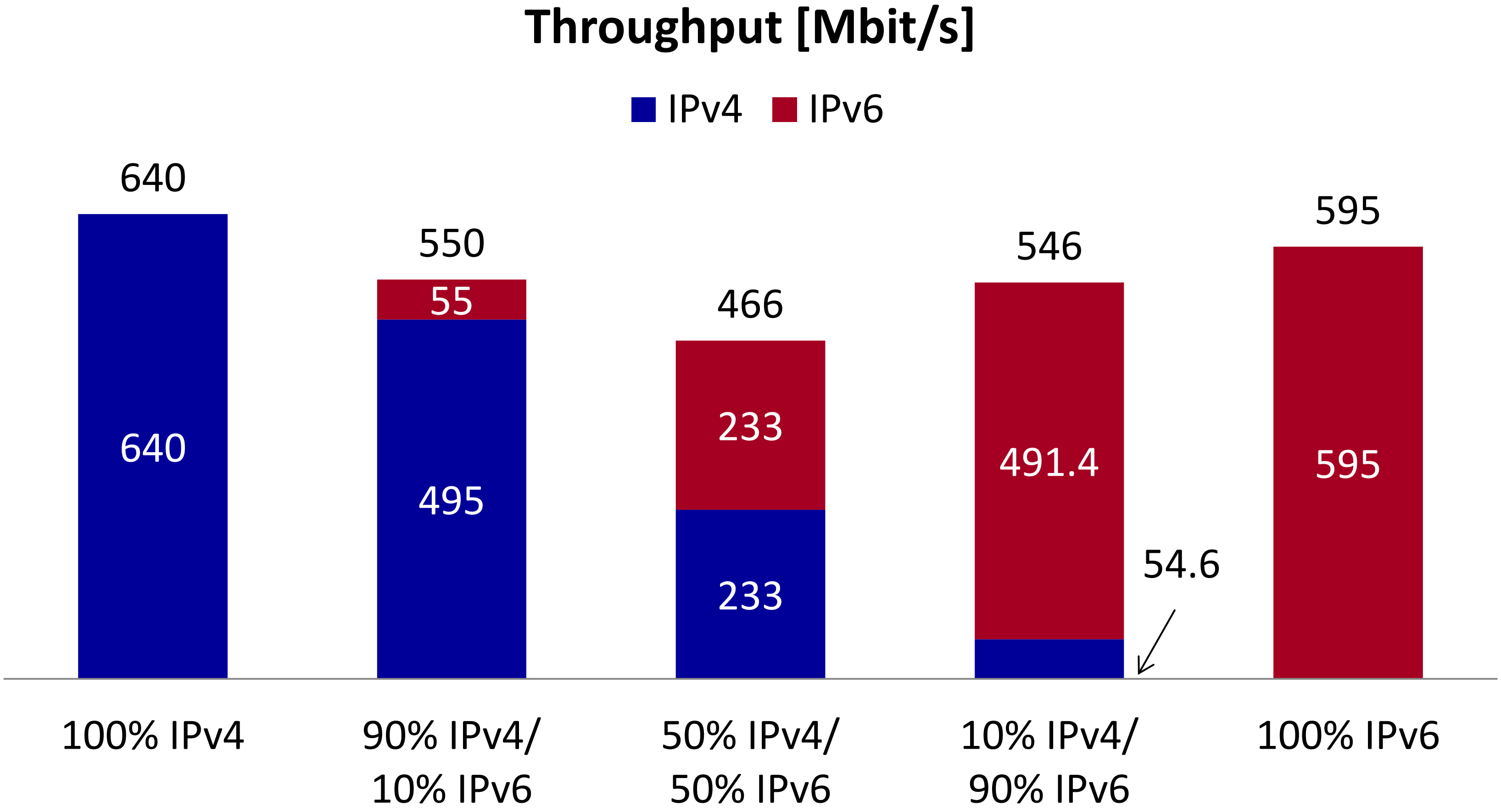
Layer 3 Throughput [Mbit/s]
Checkpoint CP2210



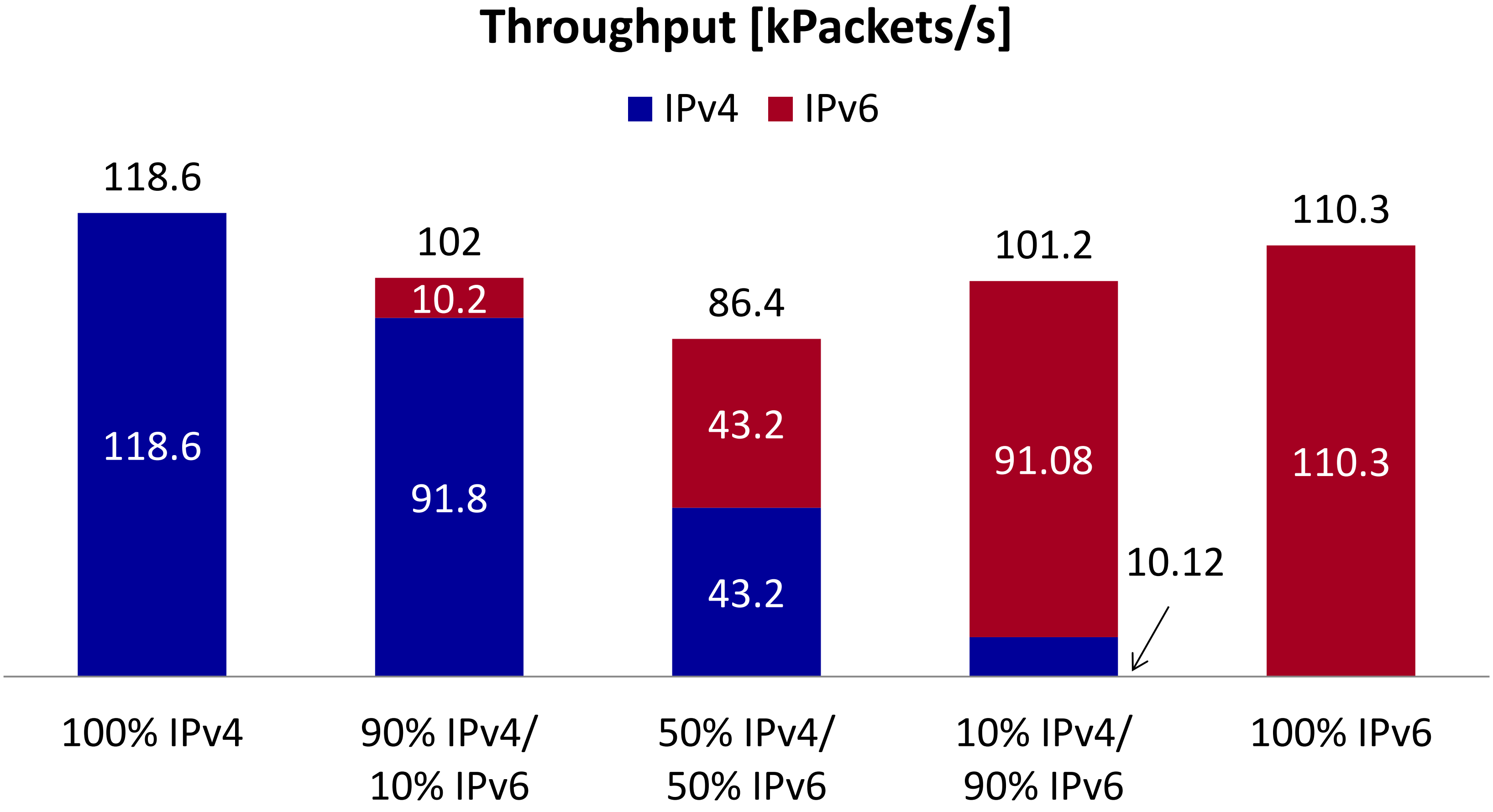
Layer 3 Throughput [kPackets/sec]
Checkpoint CP2210



Layer 3 Throughput [Mbit/s]
Juniper J2320

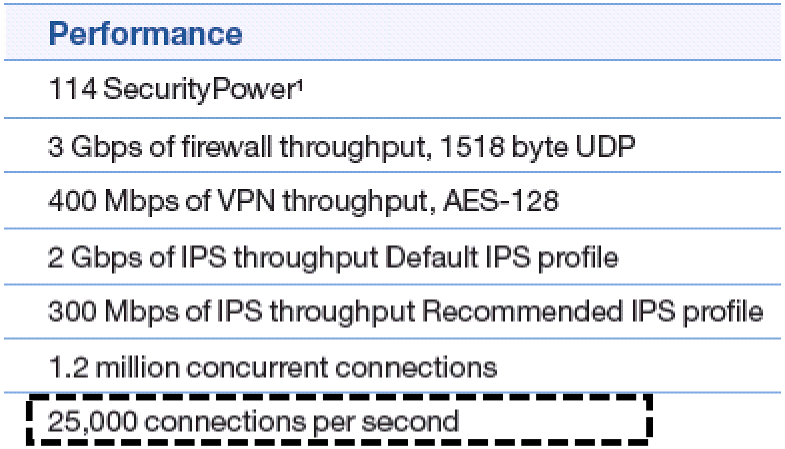


Layer 3 Throughput [kPackets/sec]
Juniper J2320



Connection Setup Rate
Checkpoint CP2210

- Measured a rate considerably lower than the vendor‘s specifications.



Performance
114 SecurityPower[1]
3 Gbps of firewall throughput, 1518 byte UDP
400 Mbps of VPN throughput, AES-128
2 Gbps of IPS throughput Default IPS profile
300 Mbps of IPS throughput Recommended IPS profile
1.2 million concurrent connections
25,000 connections per second

- Reason: Accelaration feature is disabled because of IPv6 Addresses.

Connection Setup Rate
Checkpoint CP2210 (SecureXL, 1/2)

- When the first rule contains IPv4 and IPv6 Addresses:

```
[cp2200]# fwaccel stat
Accelerator Status : on
Accept Templates : disabled by Firewall
                   disabled from rule #1
```

Measured: ca. 3.200 Connetions/s (IPv4 only)

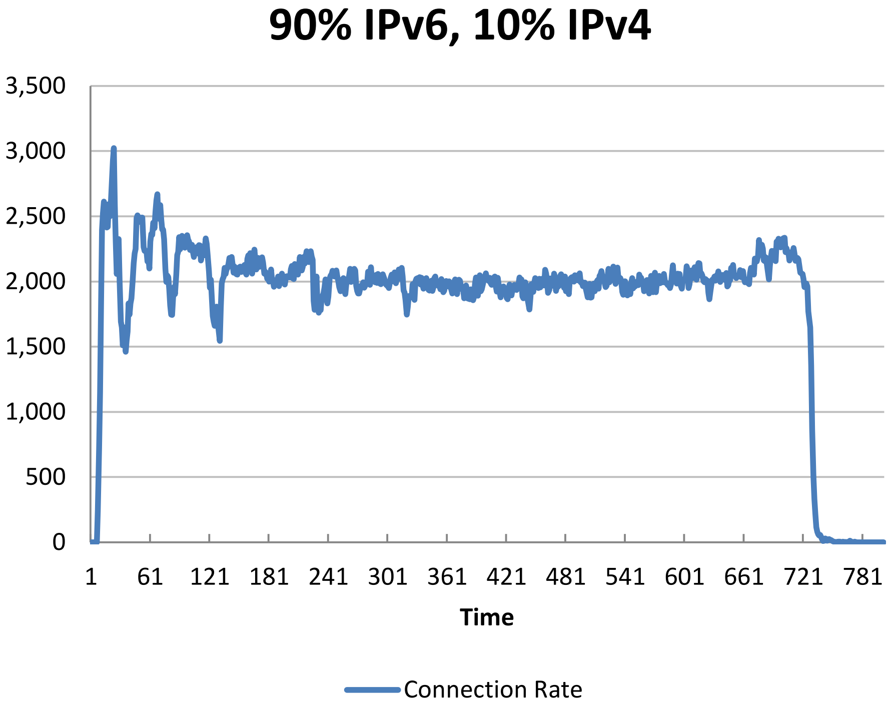
Connection Setup Rate
Checkpoint CP2210 (SecureXL, 2/2)

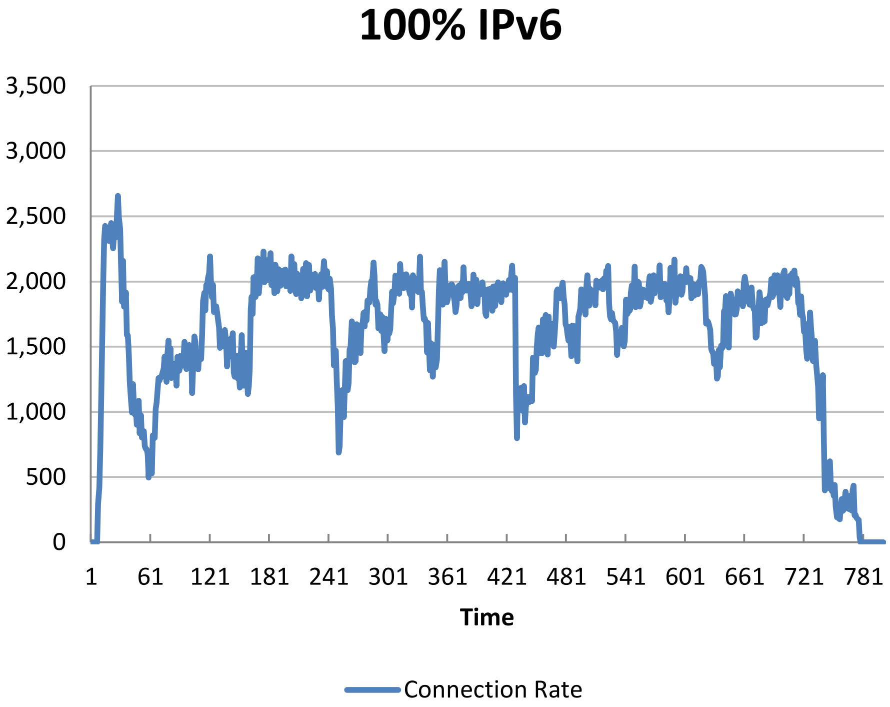
- After removing IPv6 Addresses from the first rule:

```
[cp2200]# fwaccel stat
Accelerator Status : on
Accept Templates : disabled by Firewall
                   disabled from rule #4
```

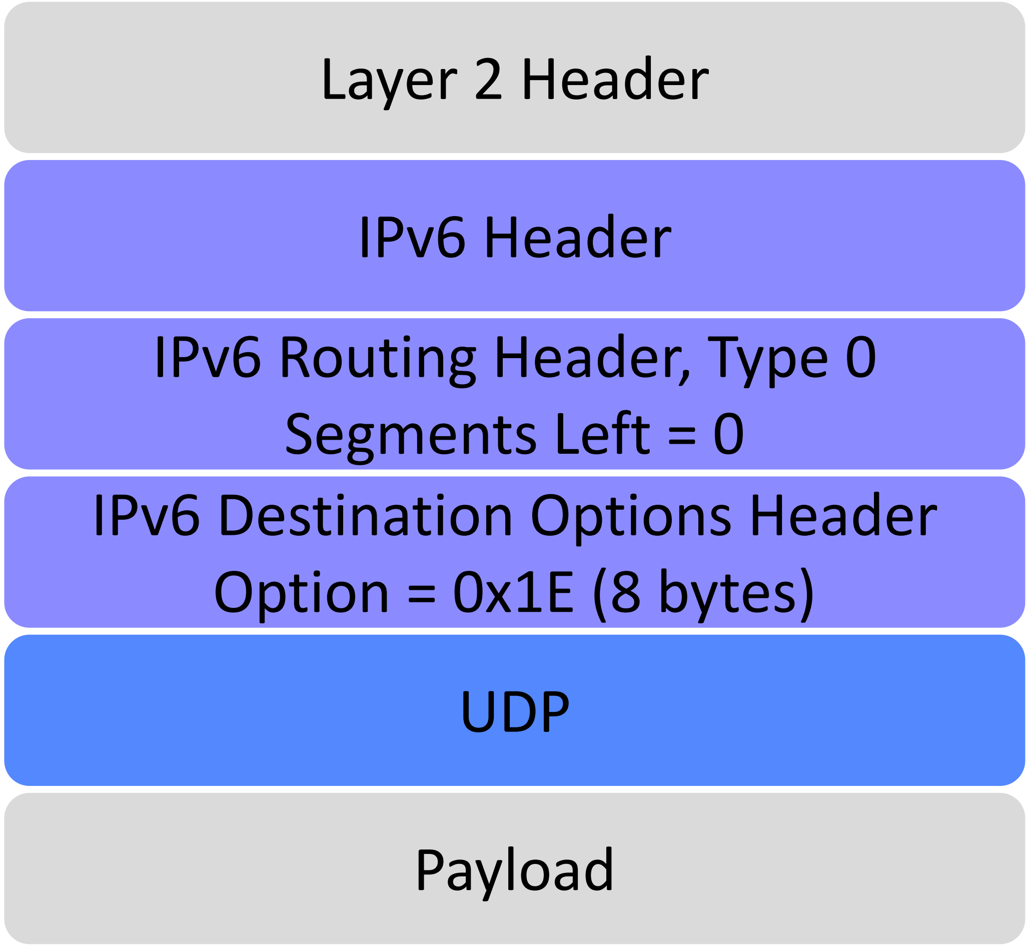
Measured: ca. 17.000 Connections/s (IPv4 only)

Connection Setup Rate
Checkpoint CP2210 (Results)





Layer 3 Throughput with Extension Headers Header Layout (1/2)



Layer 2 Header

IPv6 Header

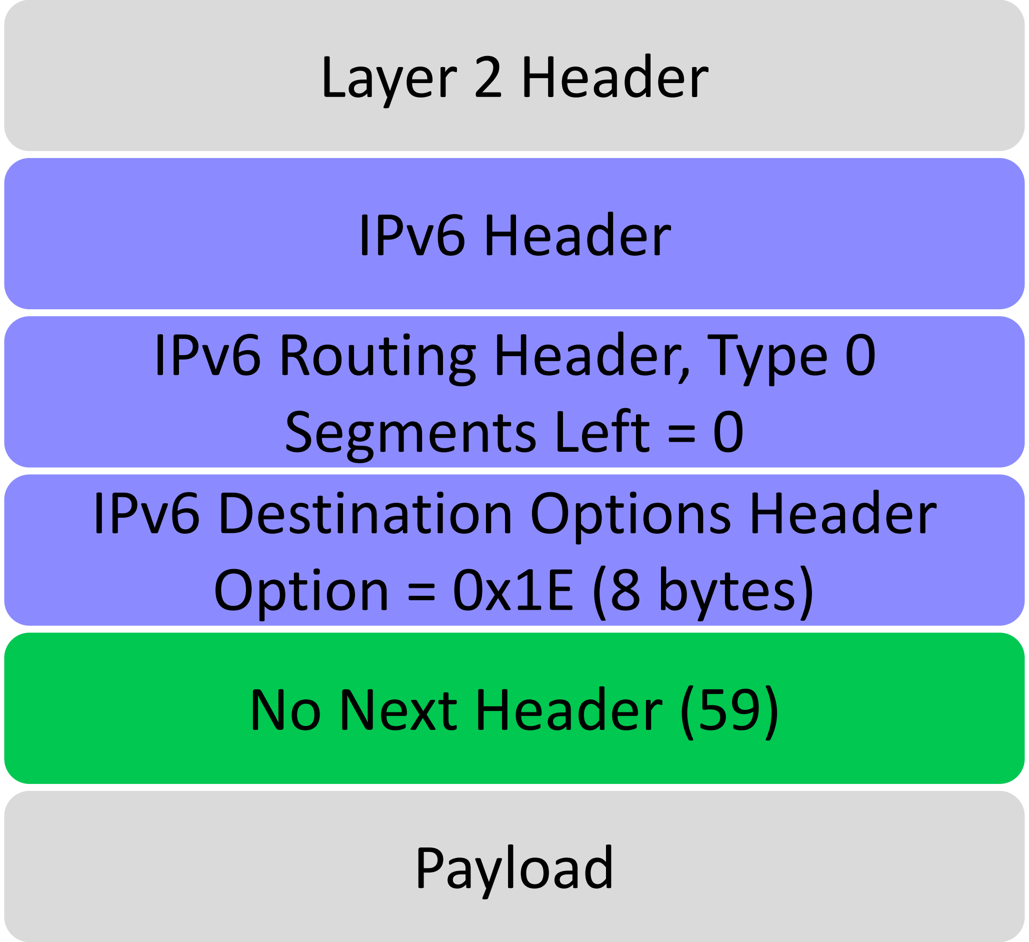
IPv6 Routing Header, Type 0
Segments Left = 0

IPv6 Destination Options Header
Option = 0x1E (8 bytes)

UDP

Payload

Layer 3 Throughput with Extension Headers Header Layout (2/2)



Layer 2 Header

IPv6 Header

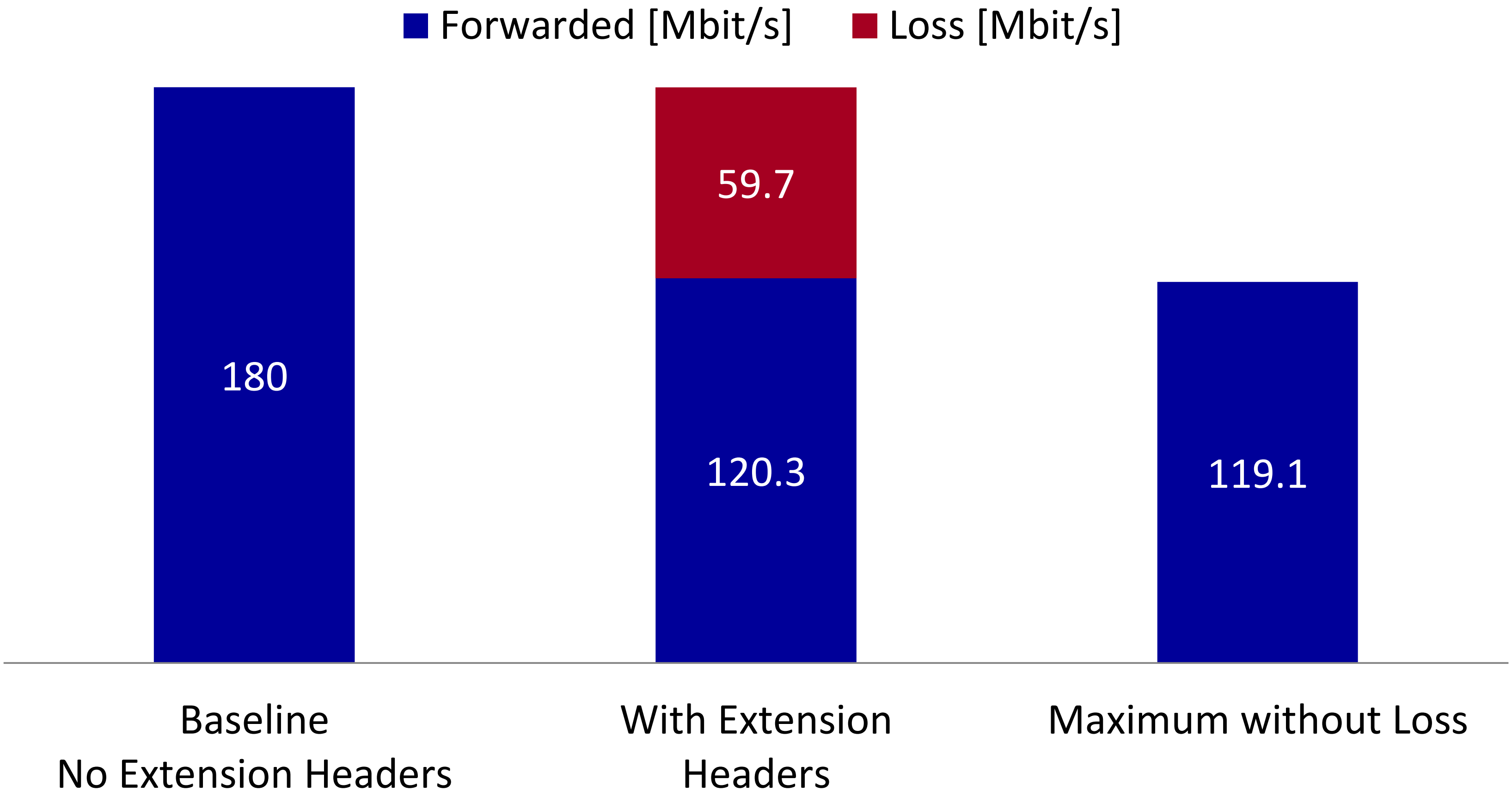
IPv6 Routing Header, Type 0
Segments Left = 0

IPv6 Destination Options Header
Option = 0x1E (8 bytes)

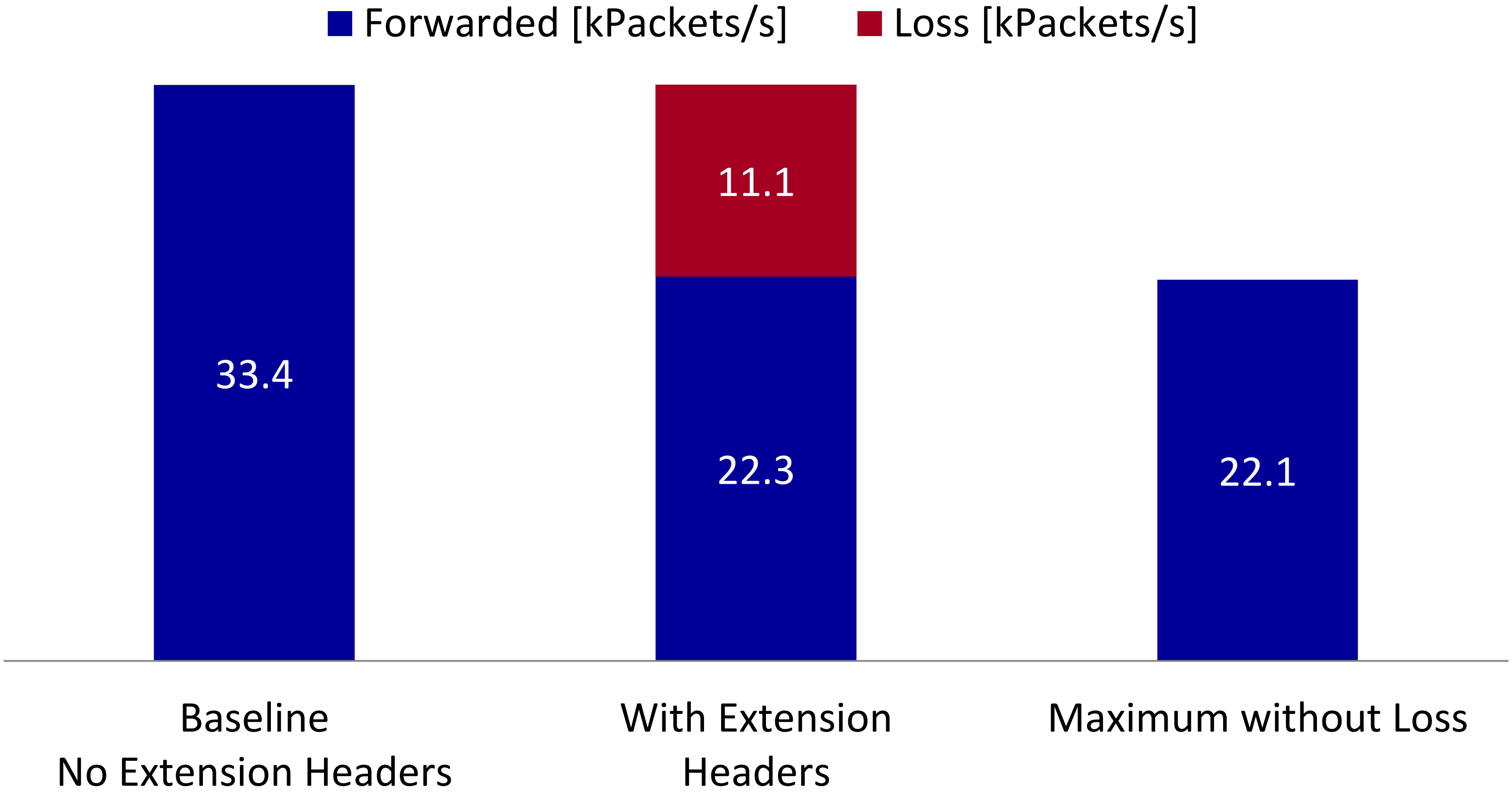
No Next Header (59)

Payload

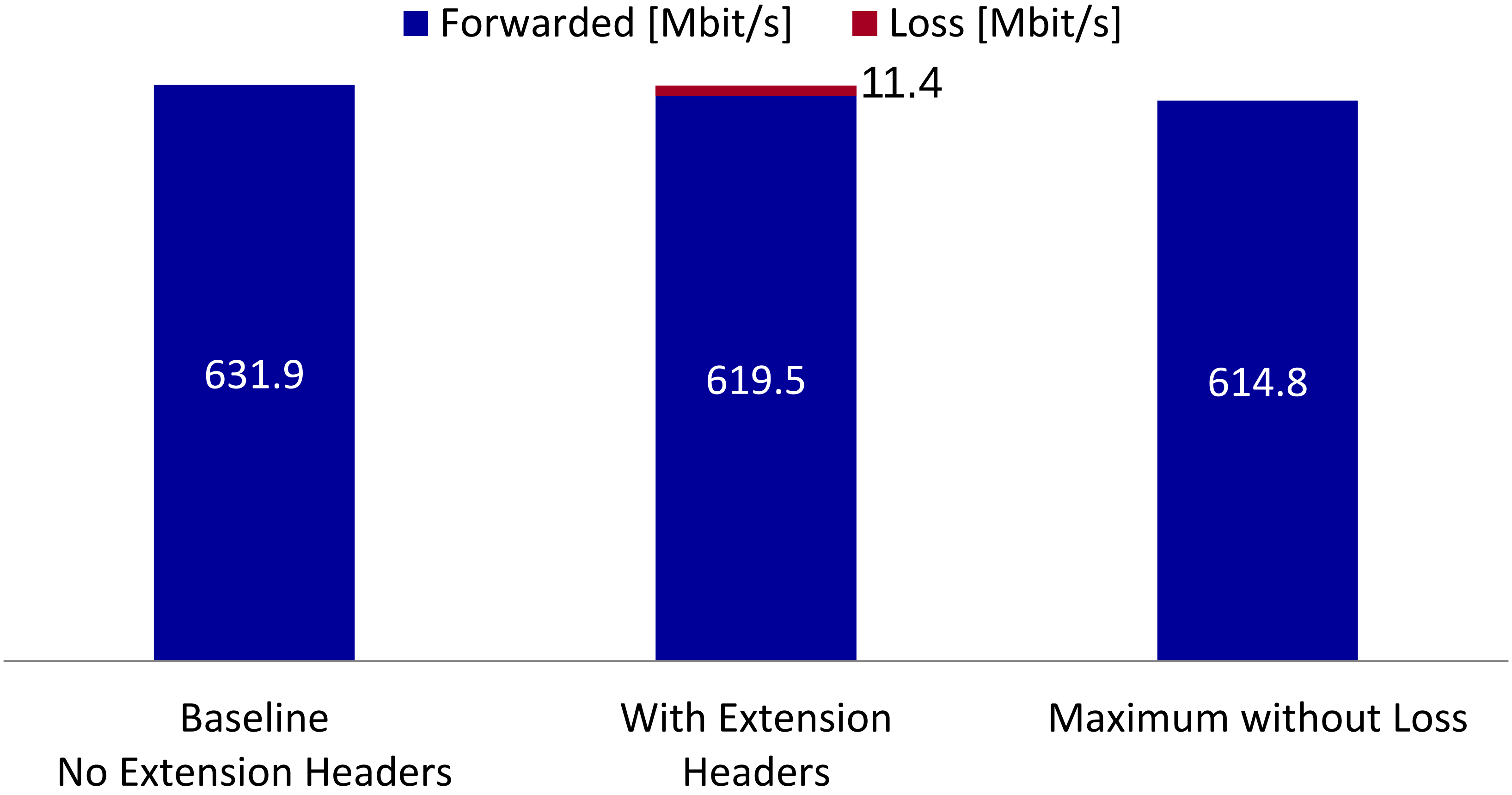
Layer 3 Throughput with Extension Headers Checkpoint CP2210 [Mbit/sec]



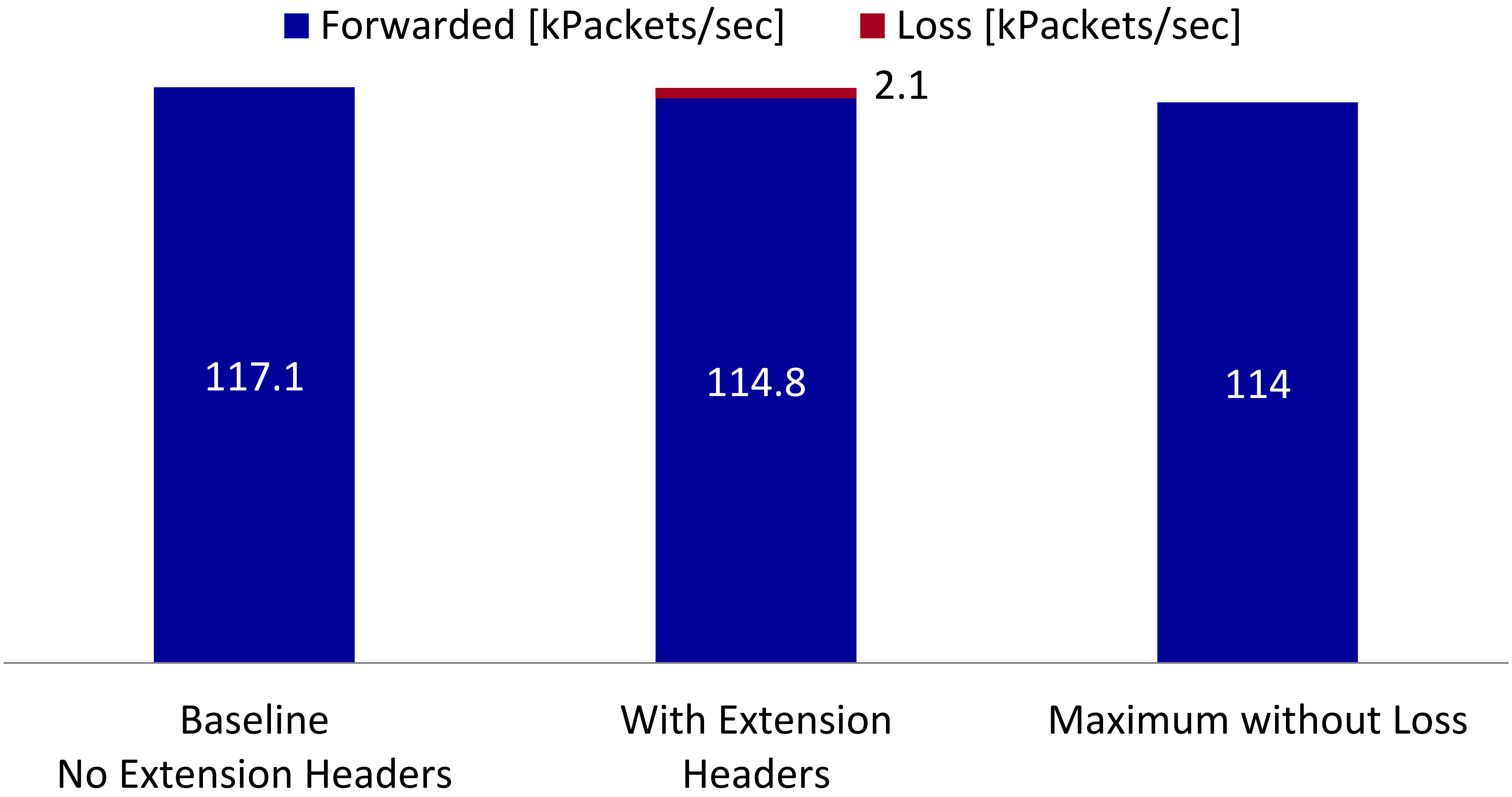
Layer 3 Throughput with Extension Headers Checkpoint CP2210 [kPackets/sec]



Layer 3 Throughput with Extension Headers Juniper J2320 [Mbit/sec]



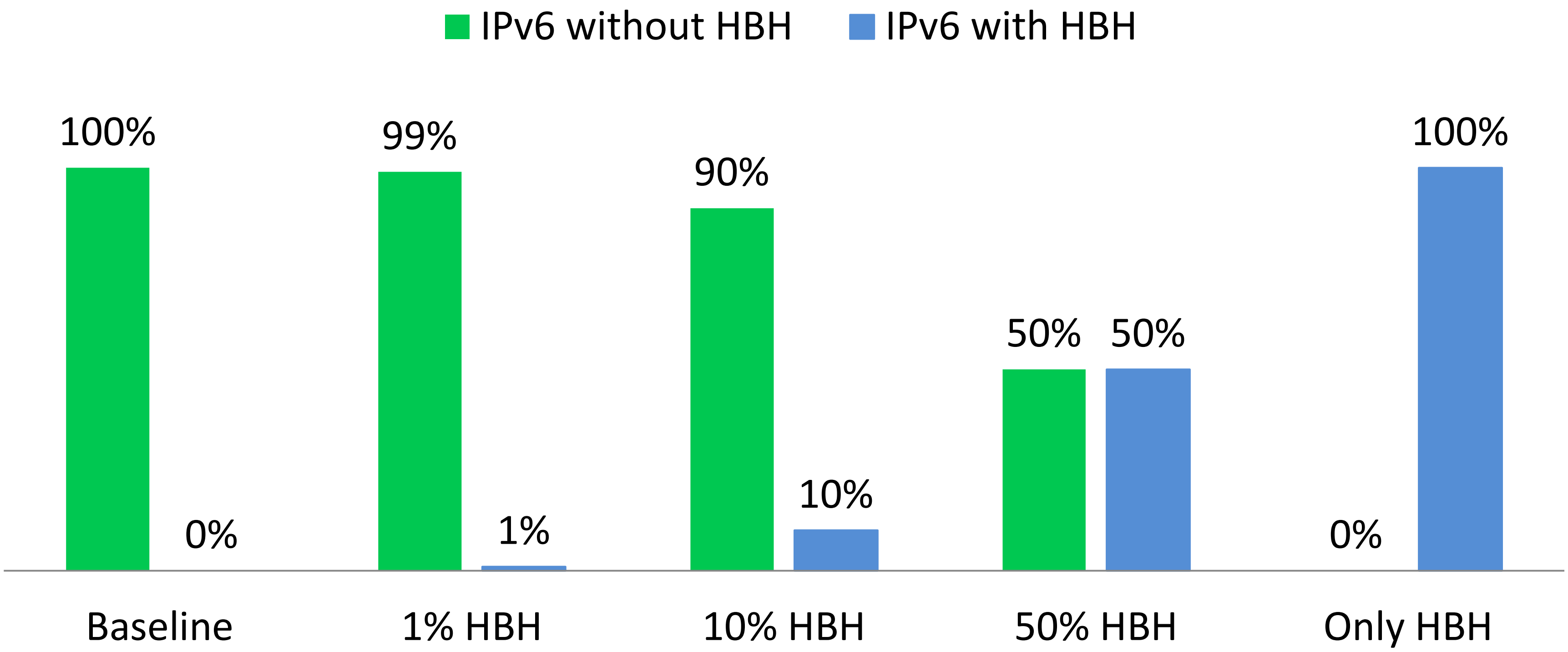
Layer 3 Throughput with Extension Headers Juniper J2320 [kPackets/sec]



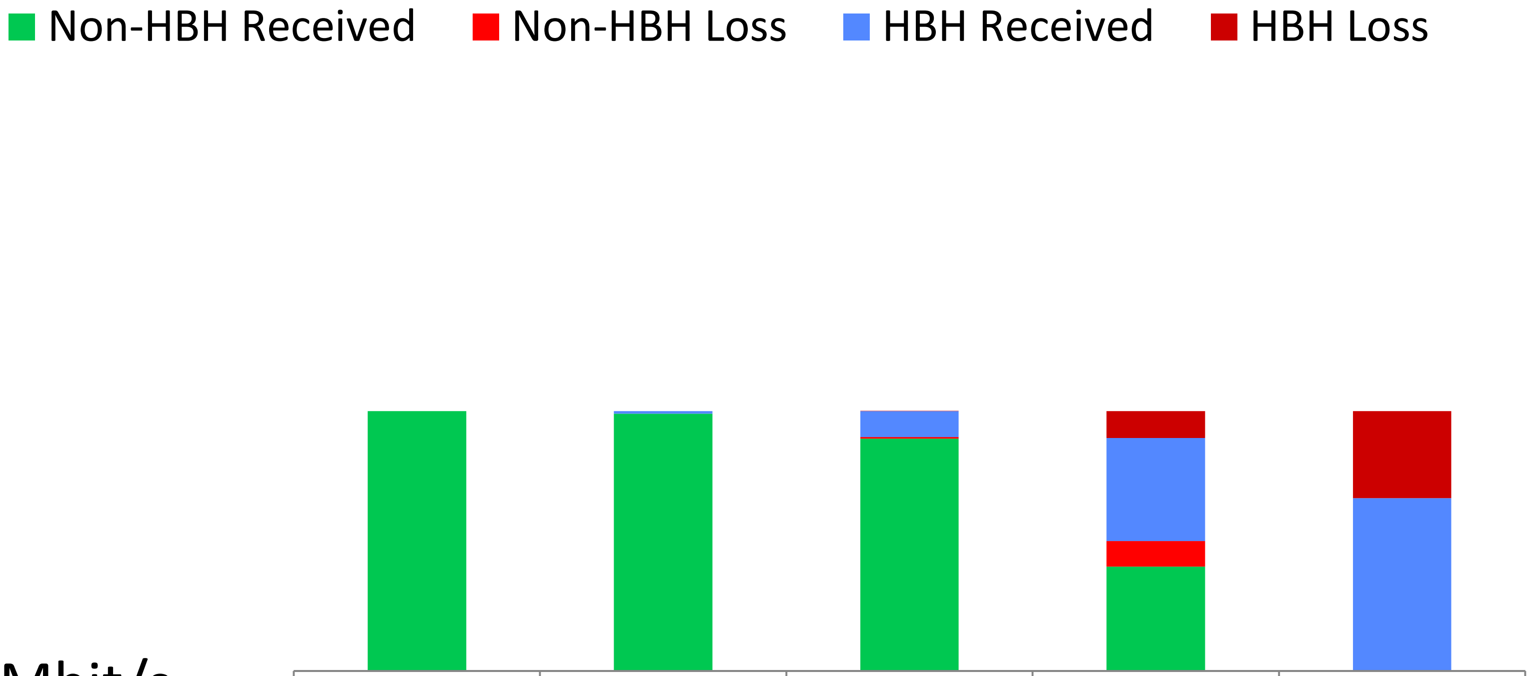
Layer 3 Throughput with Hop-by-Hop Options Header

- Possible performance impact for Hop-by-Hop (HBH) Options

  Indicated by IETF RFC 5180.

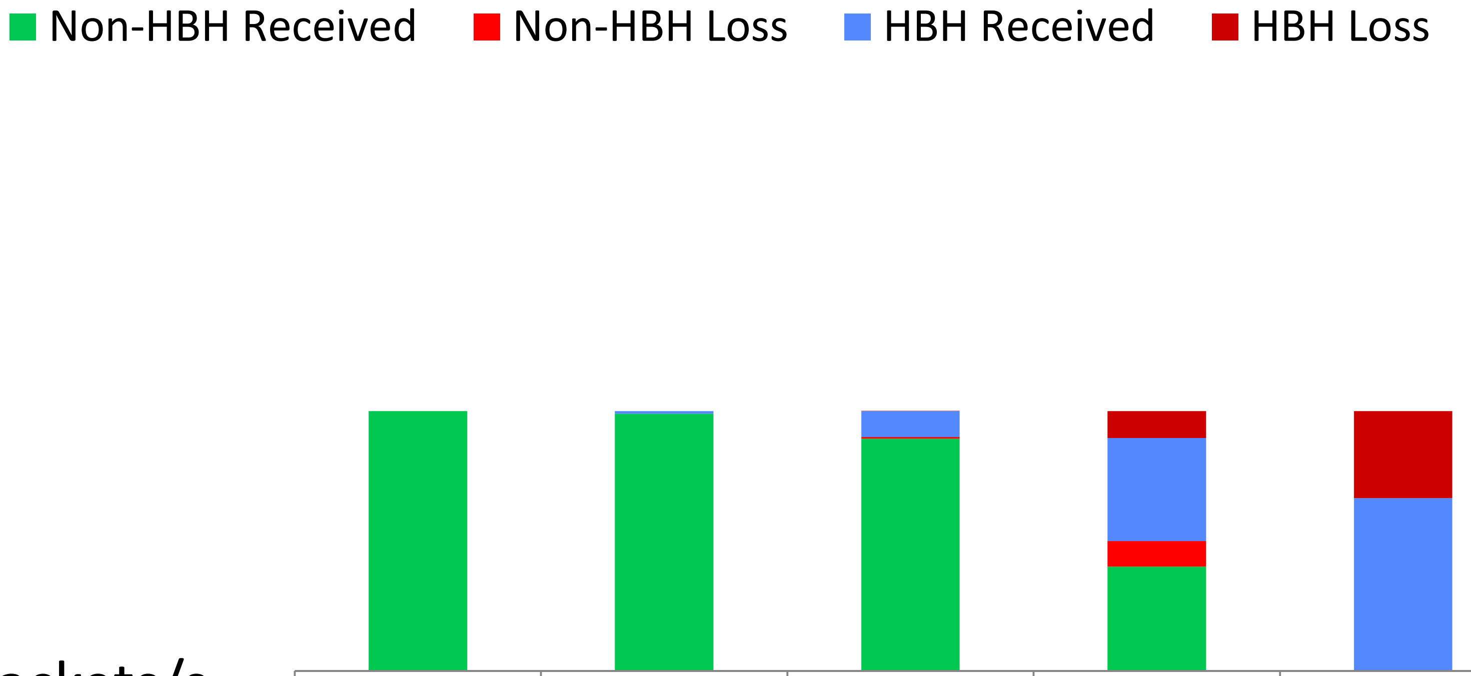


Hop-by-Hop Extension Headers
Checkpoint CP2210



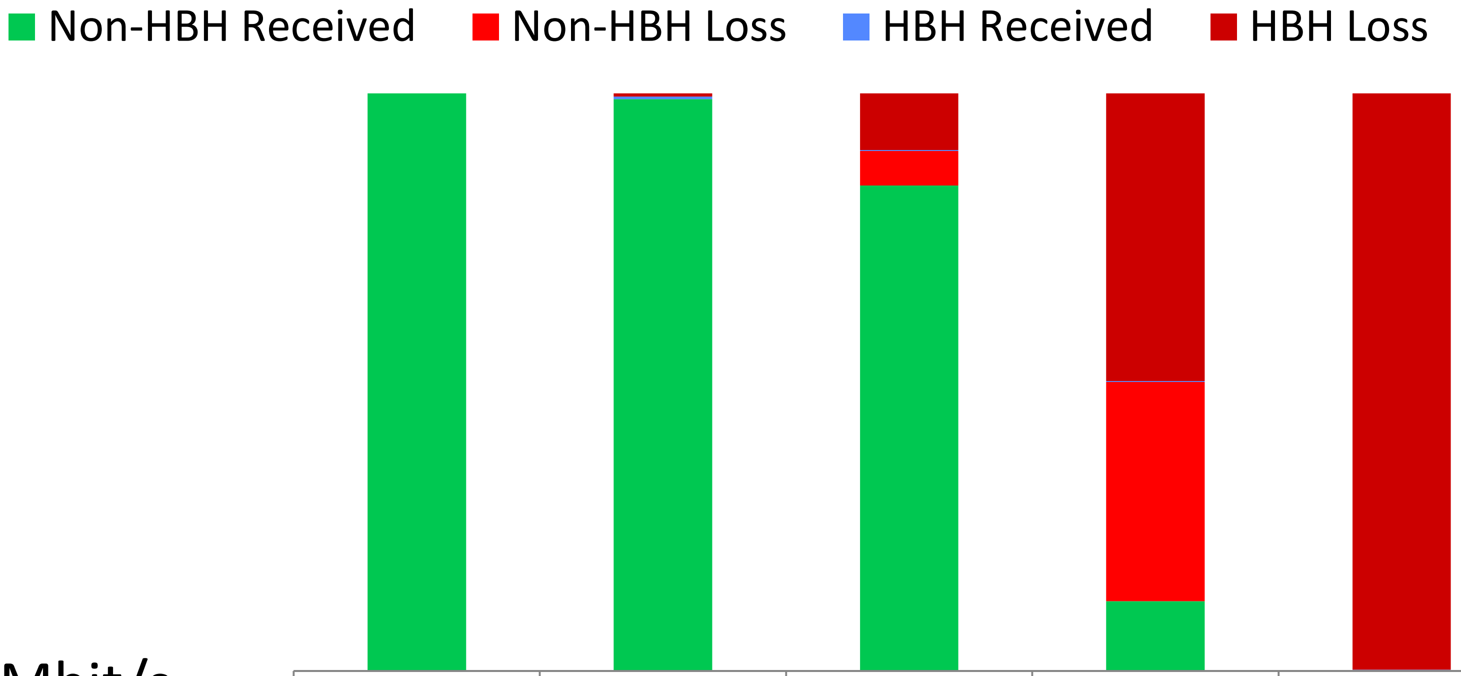
Mbit/s	Baseline	1% HBH	10% HBH	50% HBH	Only HBH
HBH Loss		0	0.108	18.72	60.3
HBH Received		1.8	17.892	71.28	119.7
Non-HBH Loss	0	0	1.134	17.73	
Non-HBH Received	180	178.2	160.866	72.27	

Hop-by-Hop Extension Headers
Checkpoint CP2210



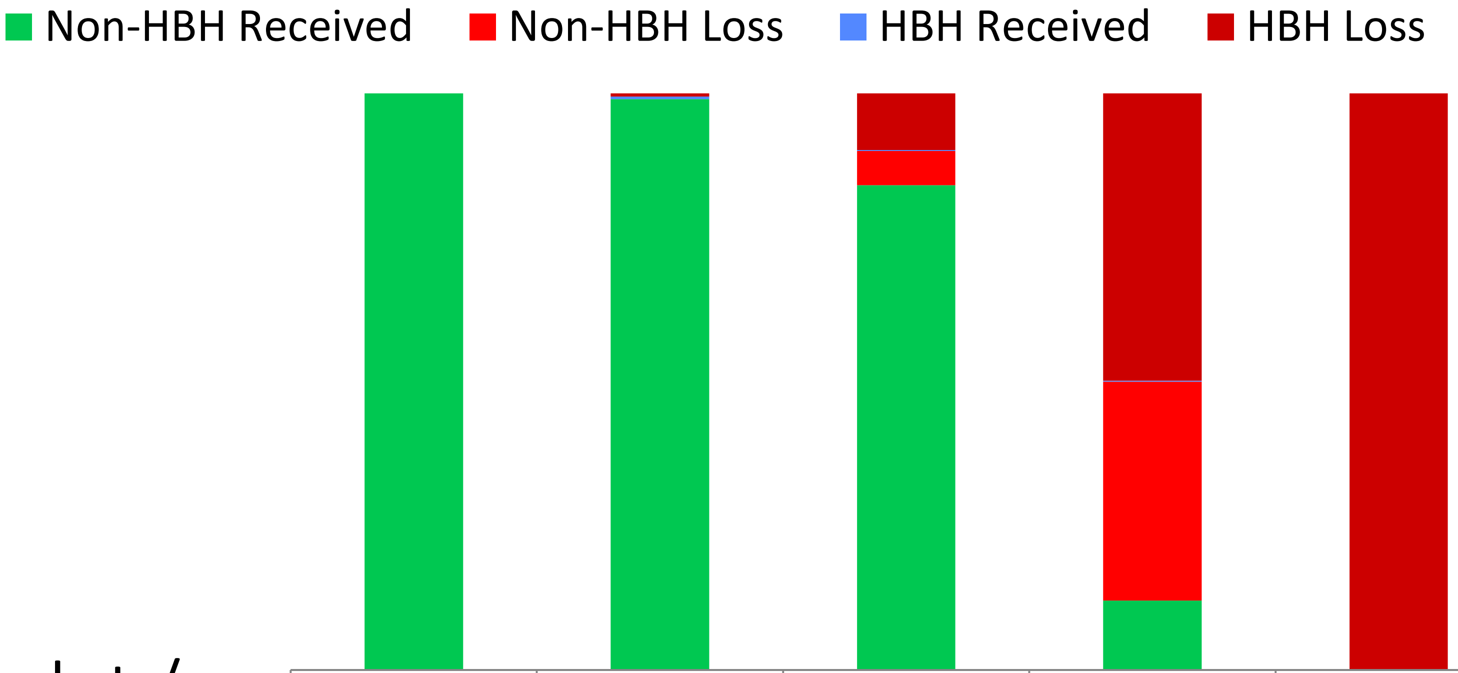
Packets/s	Baseline	1% HBH	10% HBH	50% HBH	Only HBH
HBH Loss		0	20	3470.3	11178.3
HBH Received		333.7	3316.8	13213.7	22189.7
Non-HBH Loss	0	0	210.3	3286.8	
Non-HBH Received	33367.9	33034.3	29820.9	13397.2	

Hop-by-Hop Extension Headers
Juniper J2320



Mbit/s	Baseline	1% HBH	10% HBH	50% HBH	Only HBH
HBH Loss		2.204	39.2	199.2	399.2
HBH Received		1.796	0.8	0.8	0.8
Non-HBH Loss	0	0	23.76	151.8	
Non-HBH Received	400	396	336.24	48.2	

Hop-by-Hop Extension Headers
Juniper J2320



Packets/s	Baseline	1% HBH	10% HBH	50% HBH	Only HBH
HBH Loss		408.6	7266.8	36927.2	74002.7
HBH Received		332.9	148.3	148.3	148.3
Non-HBH Loss	0	0	4404.6	28140.3	
Non-HBH Received	74,151	73409.5	62331.3	8935.2	

Questions?

Thank you for your interest!

For further information, please contact us:

EANTC AG
Salzufer 14
D-10587 Berlin
Germany

Phone: +49.30.318 05 95-0
Fax: +49.30.318 05 95-10
E-mail: info@eantc.de
www.eantc.de