AWK GROUP

Consulting
Engineering
Project Management

IoT to Gateway

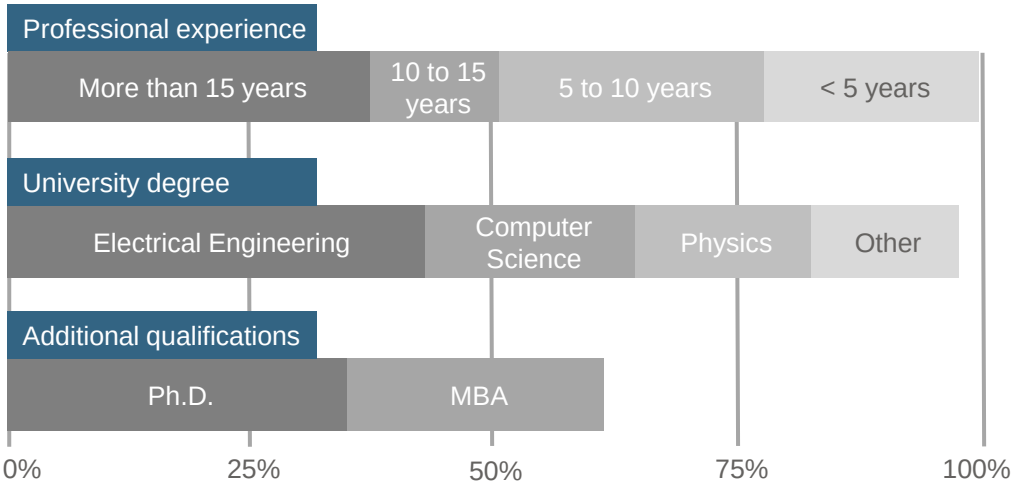
Troopers, March 20th, 2017

Gabriel Müller, Senior Consultant

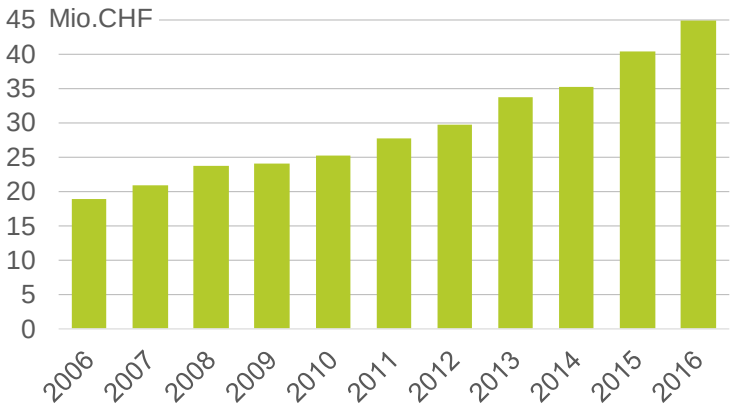
Facts and Figures

Activity	Consulting, engineering und project management for information technology from a single source
Owner	The share capital is wholly owned by the partners
Founded in	1986
Employees	Over 200 staff
Clients	Over 400
Projects	Over 4‘000
Site Locations	Zurich, Berne, Basle, Lausanne

Qualification of our Consultants



Turnover



Partners of AWK

From left to right:
Ralph Tonezzer,
Peter Gabriel,
Kurt Biri,
Christian Mauz,
Oliver Vaterlaus
(Managing Partner),
Ueli Sandmeier,
André Arrigoni

Contents

Internet of Things

Internet of Things

Characteristics

- Autonomous machine to machine communication / data exchange
- Often the Internet is used as ‘transport’ network

Examples

- Sensor networks
- Home automation
- Amazon button

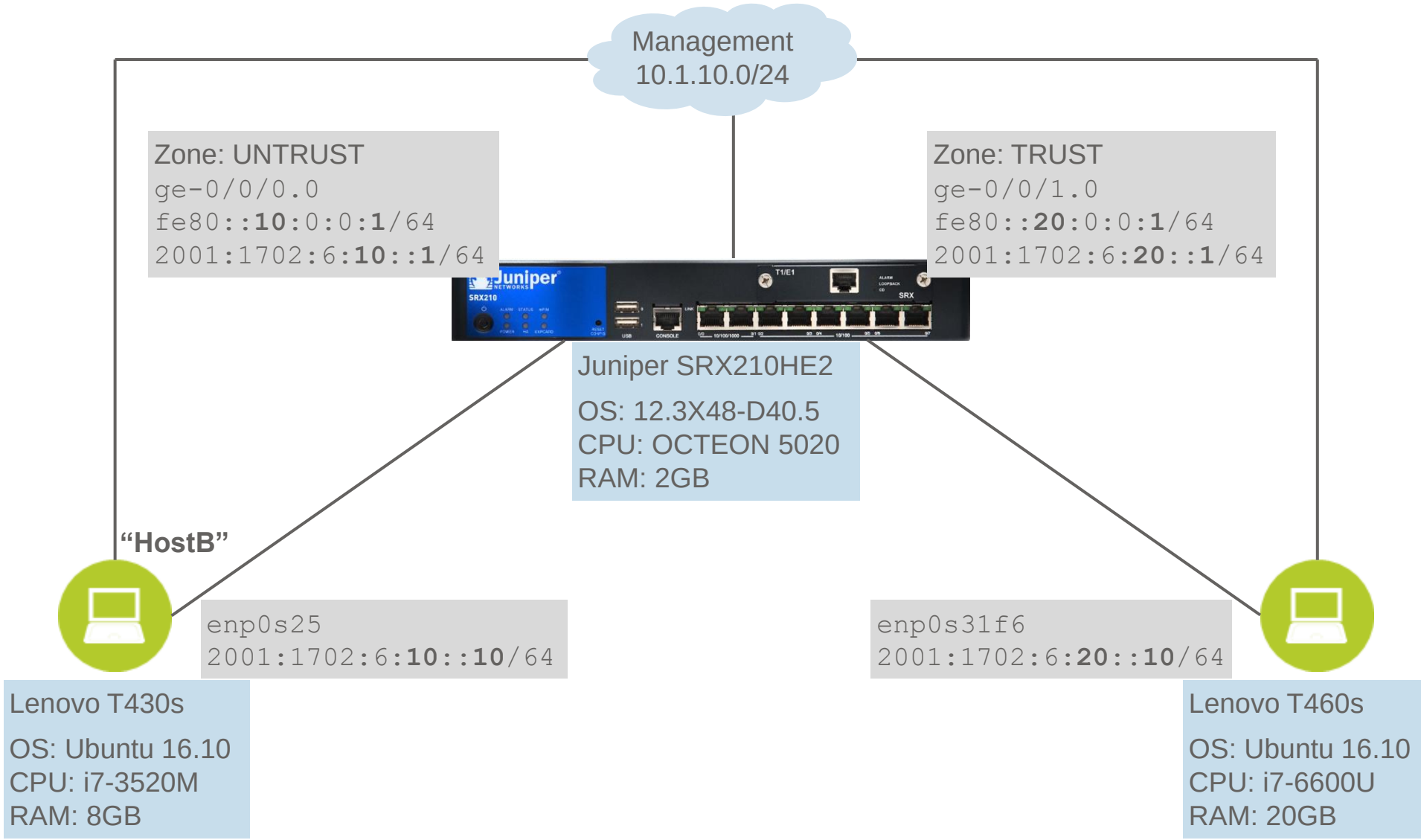
Source: amazon.com

Motivation for this talk

- Assumption: Most often some kind of ‘centralized’ access to the Internet required
- Curious about resource consumption on centralized access point (router/firewall)
- Focus on address assignment, DNS and neighbour cache

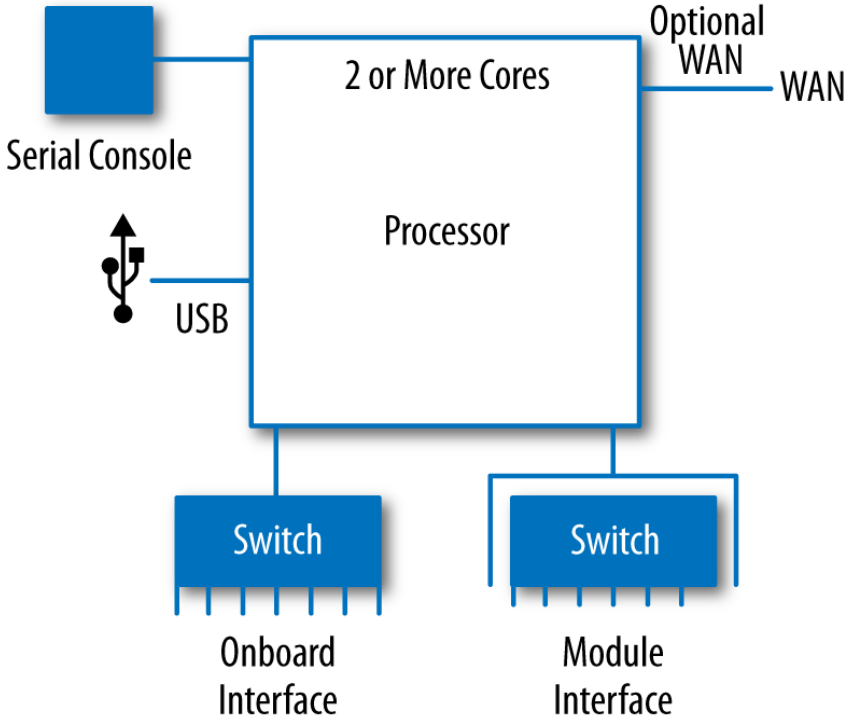
Contents

The Big Picture



Juniper SRX-210HE Details

- Juniper SRX Branch Architecture
  - No dedicated hardware for control and data plan (all on same processor)
    - Dedicated core(s) for control plane
    - Dedicated core(s) for data plane
- SRX-210HE2
  - CAVIUM's OCTEON 5020 CPU (MIPS)
    - 1 CPU core for control plane
    - 1 CPU core for data plane
  - 2Gbyte of RAM
    - 1Gbyte for control plane
    - 1Gbyte for data plane
- Commands
  - Control plane
    - show chassis routing-engine
  - Data plane
    - show chassis forwarding fpc 0



Source: http://chimera.labs.oreilly.com

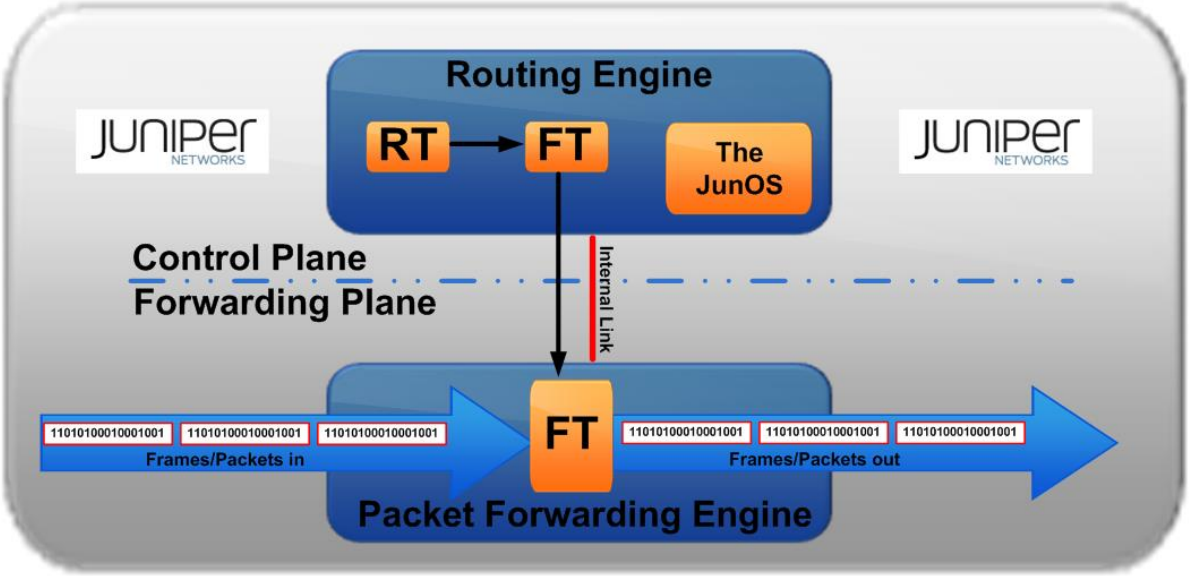
Juniper SRX-210HE Details

Routing Engine

- Protocol update
  - Bridging table
  - Routing table
  - Primary forwarding table (FT)
- System management

Packet Forwarding Engine

- Forwarding
  - Packets
  - Frames
- Advanced services
  - Policers (rate limiting)
  - Stateless firewall filters
  - Class of services



Source: http://packetsanalyzed.blogspot.ch

Contents

Test Case Overview

- T1XX: Ping flooding
  - T10x: Ping flooding with 1 session (to firewall / HostB)
  - T11x: Ping flooding with 5 sessions (to firewall / HostB)
- T12X: DNS testing
  - T121: DNS proxy on firewall
  - T122: DNS proxy on HostB
- T13X: DHCPv6 testing
  - T131: DHCPv6 server on firewall
  - T132: DHCPv6 server on HostB (firewall as relay)

T101 – Ping Flood Firewall – 1 Session

1 session

```
root@T460s:/home/muellega# ping6 2001:1702:6:20::1
PING 2001:1702:6:20::1(2001:1702:6:20::1) 56 data bytes
--- 2001:1702:6:20::1 ping statistics ---
51 packets transmitted, 51 received, 0% packet loss, time 50070ms rtt
min/avg/max/mdev = 1.710/2.284/12.386/1.437 ms
root@T460s:/home/muellega#
```

Doing the math: 1/0.002284sec = ~438 pings per second

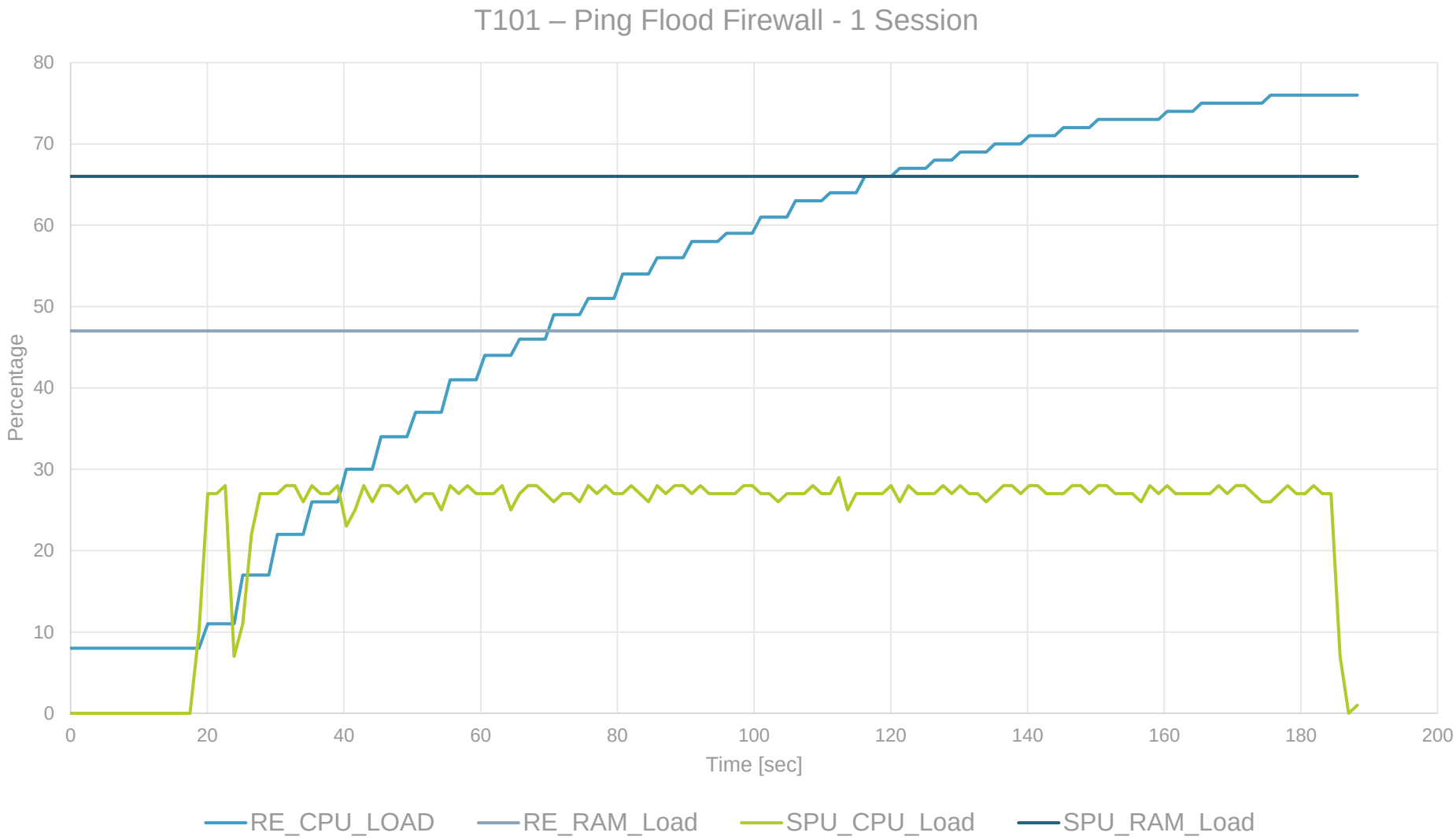
```
root@T460s:/home/muellega# ping6 -f 2001:1702:6:20::1
PING 2001:1702:6:20::1(2001:1702:6:20::1) 56 data bytes...^C
--- 2001:1702:6:20::1 ping statistics ---
75862 packets transmitted, 75859 received, 0% packet loss, time 167264ms rtt
min/avg/max/mdev = 1.652/2.253/453.300/5.774 ms, pipe 29, ipg/ewma 2.204/2.150 ms
root@T460s:/home/muellega#
```

Doing the math again:

- 75862 / 167.264sec = ~453 pings per second
- Compare with SNMP data: Average SPU_SessIPv6_96Sec: 463

T101 – Ping Sweep Firewall – 1 Session – Load

1 session



T102 – Ping Flood HostB - 1 Session (over Firewall)

1 session

```
root@T460s:/home/muellega# ping6 2001:1702:6:10::10
PING 2001:1702:6:10::10(2001:1702:6:10::10) 56 data bytes
--- 2001:1702:6:10::10 ping statistics ---
58 packets transmitted, 58 received, 0% packet loss, time 57243msrtt
min/avg/max/mdev = 0.733/0.913/1.166/0.091 ms
root@T460s:/home/muellega#
```

Doing the math: 1/0.000913sec = ~1095 pings per second

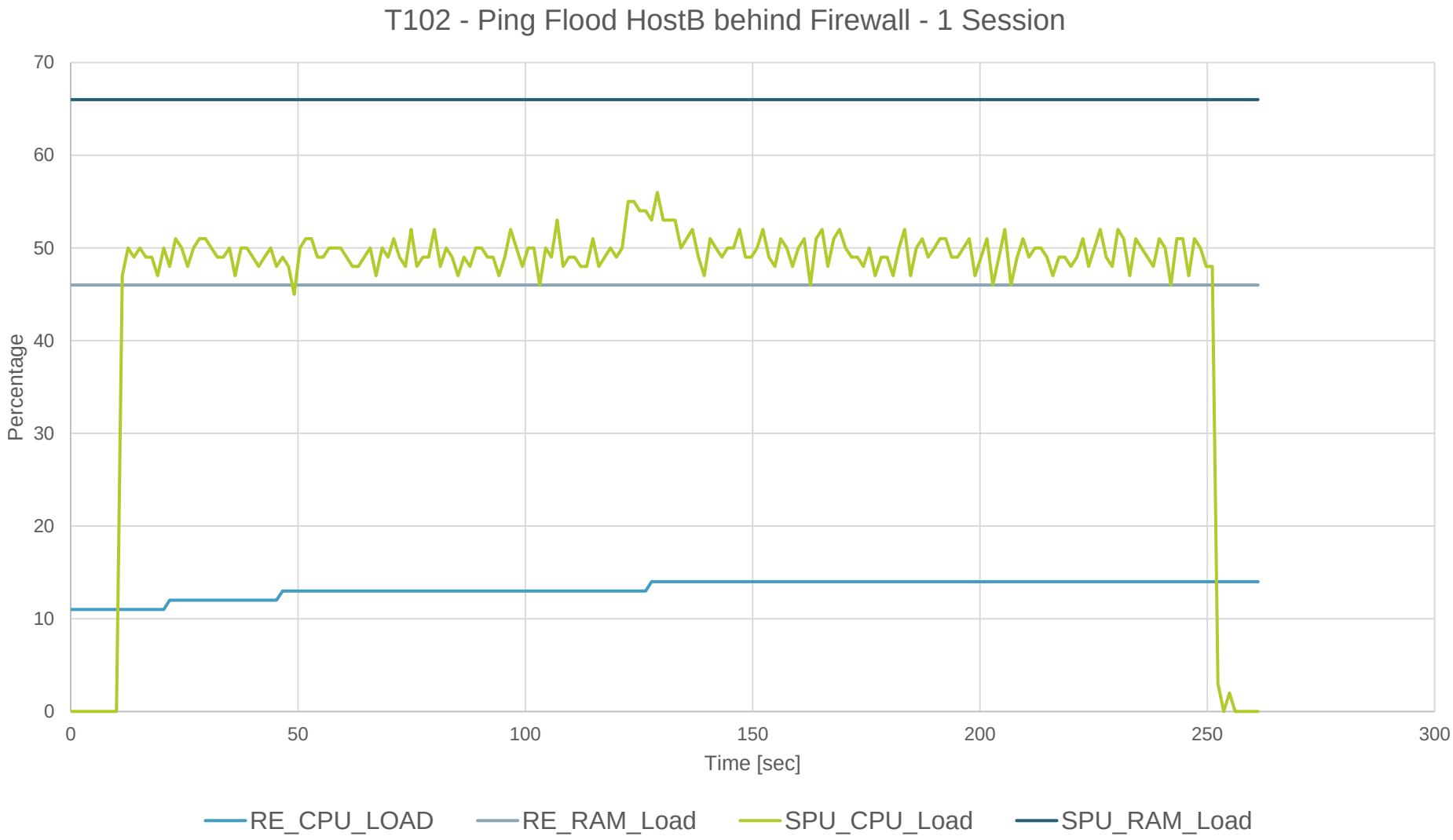
```
root@T460s:/home/muellega# ping6 -f 2001:1702:6:10::10
PING 2001:1702:6:10::10(2001:1702:6:10::10) 56 data bytes
--- 2001:1702:6:10::10 ping statistics ---
298972 packets transmitted, 298972 received, 0% packet loss, time 240650ms
rtt min/avg/max/mdev = 0.475/0.732/26.532/0.562 ms, pipe 2, ipg/ewma 0.804/0.726
msroot@T460s:/home/muellega#
```

Doing the math again:

- 298972 / 240.650sec = ~1242 pings per second
- Compare with SNMP data: Average SPU_SessIPv6_96Sec: 1243

T102 – Ping Flood HostB – 1 Session (over Firewall) – Load

1 session



T111 – Ping Flood Firewall – 5 Sessions

5 sessions

Starting 5 ping flood sessions in parallel

Results:

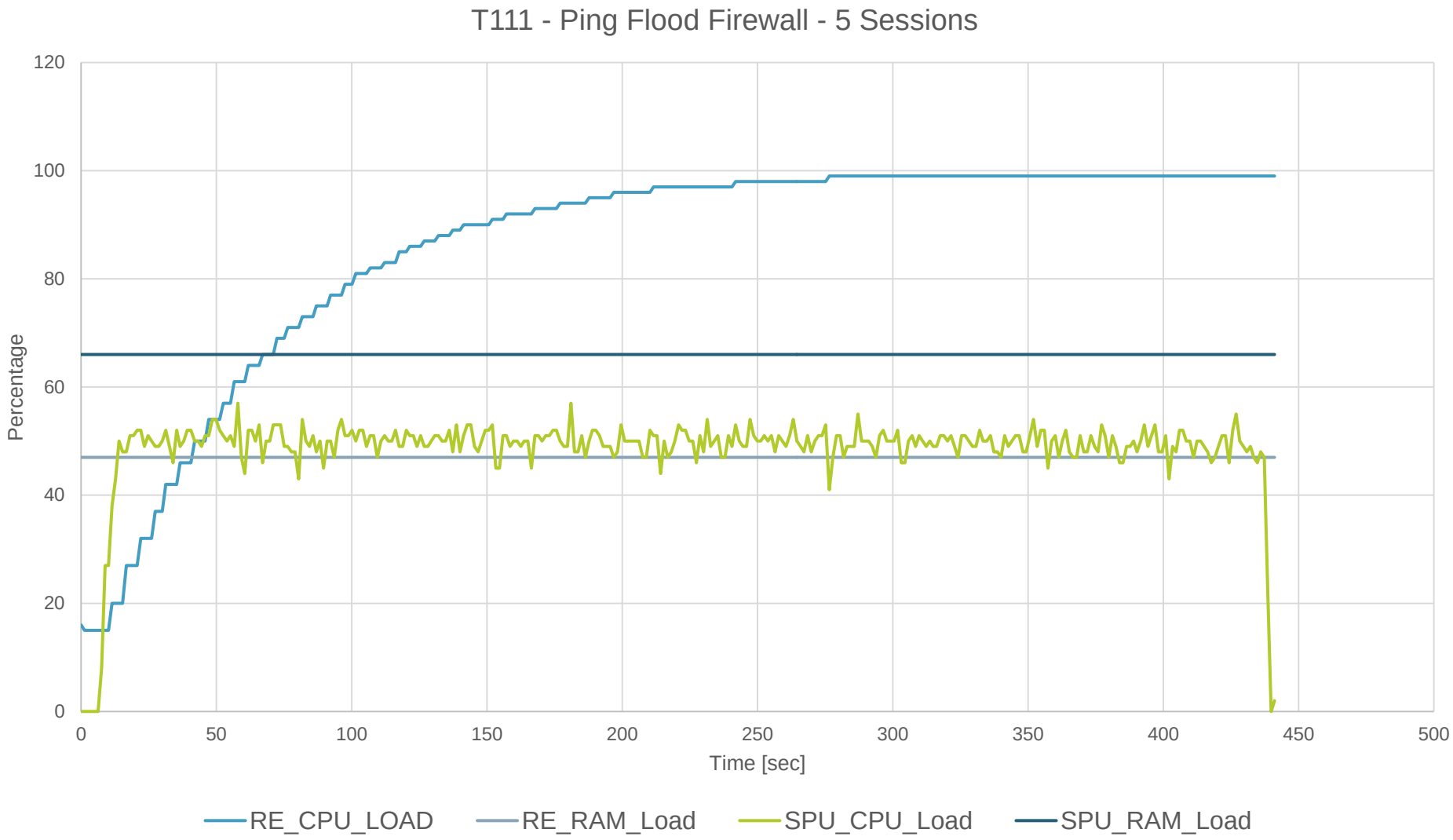
```
rtt min/avg/max/mdev = 1.686/5.027/211.652/3.493 ms, pipe 13, ipg/ewma 4.973/4.276 ms
rtt min/avg/max/mdev = 1.893/5.066/223.292/3.496 ms, pipe 14, ipg/ewma 5.008/3.366 ms
rtt min/avg/max/mdev = 1.768/5.071/223.323/3.478 ms, pipe 14, ipg/ewma 5.009/2.730 ms
rtt min/avg/max/mdev = 1.725/5.062/211.616/3.500 ms, pipe 13, ipg/ewma 5.003/2.052 ms
rtt min/avg/max/mdev = 1.867/5.116/211.665/3.527 ms, pipe 13, ipg/ewma 5.052/4.647 ms
```

Doing the math again:

- 1/0.005027 + 1/0.005066 + 1/0.005071 + 1/0.005062 + 1/0.005116 = ~985
- Compare with SNMP data: Average SPU_SessIPv6_96Sec: 988

T111 – Ping Flood – 5 Sessions – Load

5 sessions



T112 – Ping Flood HostB – 5 Sessions

5 sessions

Starting 5 ping flood sessions in parallel

Results:

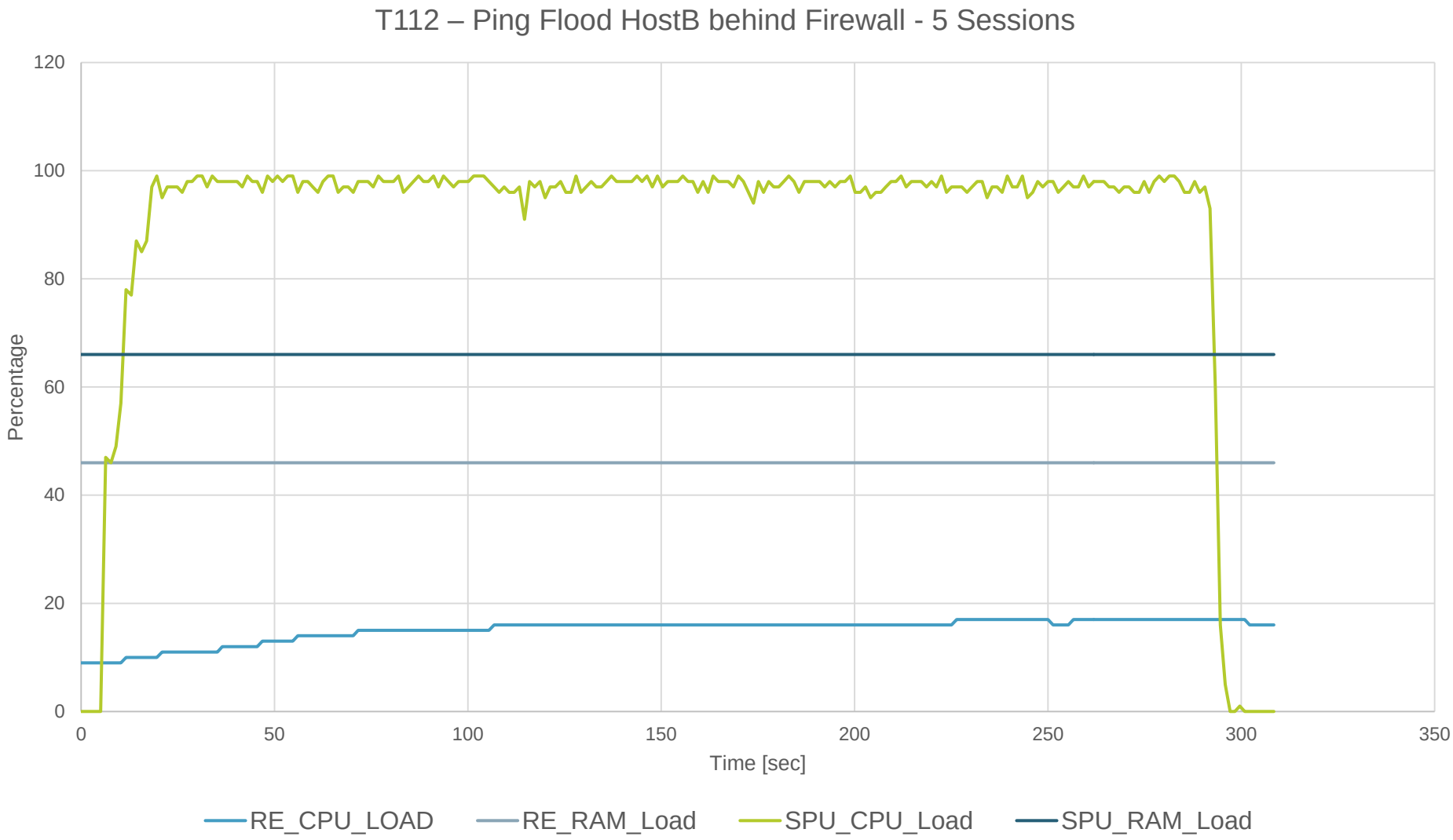
```
rtt min/avg/max/mdev = 0.472/1.847/29.609/1.341 ms, pipe 3, ipg/ewma 1.927/1.780 ms
rtt min/avg/max/mdev = 0.462/1.897/30.157/1.349 ms, pipe 3, ipg/ewma 1.978/1.383 ms
rtt min/avg/max/mdev = 0.511/1.920/30.172/1.348 ms, pipe 3, ipg/ewma 1.999/1.204 ms
rtt min/avg/max/mdev = 0.484/1.925/30.895/1.357 ms, pipe 3, ipg/ewma 2.003/0.854 ms
rtt min/avg/max/mdev = 0.479/1.920/30.167/1.350 ms, pipe 3, ipg/ewma 1.996/0.738 ms
```

Doing the math again:

- 1/0.001847 + 1/0.001897 + 1/0.001920 + 1/0.001925 + 1/0.001920 = ~2630
- Compare with SNMP data: Average SPU_SessIPv6_96Sec: 2496

T112 – Ping Flood HostB – 5 Session (over Firewall) – Load

5 sessions



T113 – Ping Flood HostB (direct) – 5 Sessions

5 sessions

Starting 5 ping flood sessions in parallel (source and destination in same network, directly connected)

Results:

```
rtt min/avg/max/mdev = 0.750/1.065/6.469/0.118 ms, ipg/ewma 1.117/1.074 ms
rtt min/avg/max/mdev = 0.752/1.066/4.783/0.114 ms, ipg/ewma 1.117/1.026 ms
rtt min/avg/max/mdev = 0.752/1.066/4.827/0.114 ms, ipg/ewma 1.116/1.023 ms
rtt min/avg/max/mdev = 0.756/1.066/6.806/0.119 ms, ipg/ewma 1.116/0.985 ms
rtt min/avg/max/mdev = 0.754/1.067/4.918/0.114 ms, ipg/ewma 1.117/0.991 ms
```

Doing the math again:

- 1/0.001065 + 1/0.001066 + 1/0.001066 + 1/0.001066 + 1/0.004067 = ~4096

T1xx – Ping – Summary

Observations Ping Flood

- RE Load vs. SPU Load
  - As expected,
    - Traffic targeting FW: RE load increases
    - Traffic passing FW: SPU load increases
- SNMP accuracy
  - Very good under normal conditions
  - T112 could indicate that accuracy suffers when SPU load is very high
- 'Throughputs' of FW and HostB (T111 and T112)
  - Makes sense when comparing CPU capacity of FW with the HostB's
- High performance when comparing to spec sheet

Product Comparison

	SRX100	SRX110	SRX210
Maximum Performance and Capacity			
Junos OS version tested	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15	Junos OS 12.1X44-D15
Firewall performance (large packets)	700 Mbps	700 Mbps	850 Mbps
Firewall performance (IMIX)	200 Mbps	200 Mbps	250 Mbps
Firewall + routing PPS (64 Byte)	70 Kpps	70 Kpps	95 Kpps
Firewall performance[8] (HTTP)	100 Mbps	100 Mbps	290 Mbps
IPsec VPN throughput (large packets)	65 Mbps	65 Mbps	85 Mbps
IPsec VPN tunnels	128	128	256
AppSecure firewall throughput[8]	90 Mbps	90 Mbps	250 Mbps
IPS (intrusion prevention system)	75 Mbps[9]	75 Mbps	65 Mbps
Antivirus	25 Mbps (Sophos AV)	25 Mbps (Sophos AV)	30 Mbps (Sophos AV)
Connections per second	1,800	1,800	2,200

Source: www.juniper.net

T121 – DNS Proxy on Firewall – DNS ALG enabled

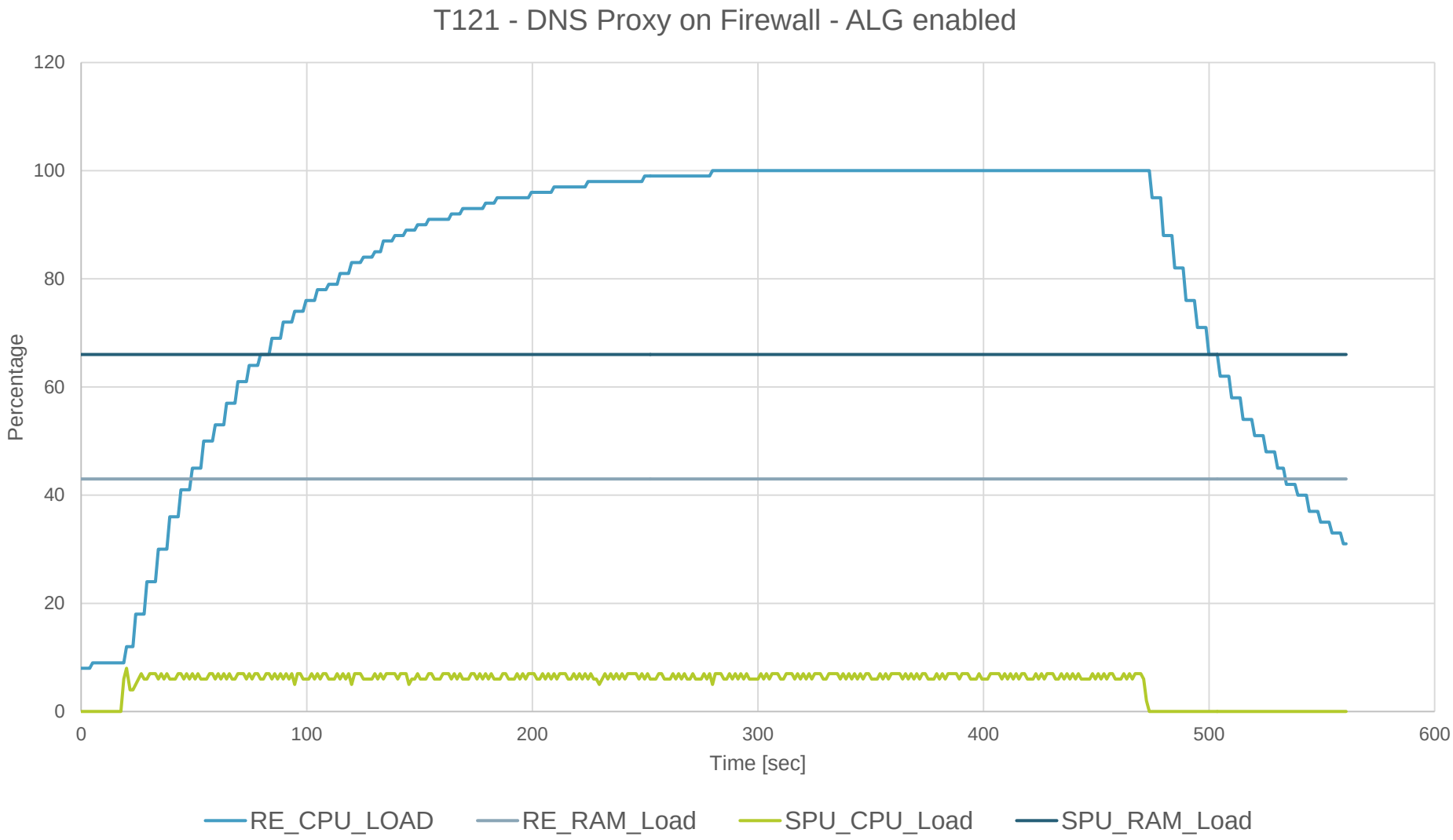
```
root@T460s:/home/muellega# ./dnsperf -s 2001:1702:6:20::1 -d input.tsv -l 600 -c 2000
DNS Performance Testing Tool Nominum
Version 2.1.0.0
[Status] Command line: dnsperf -s 2001:1702:6:20::1 -d input.tsv -l 600 -c 2000
[Status] Sending queries (to 2001:1702:6:20::1)
[Status] Started at: Tue Feb 14 12:56:17 2017
[Status] Stopping after 600.000000 seconds...

Statistics:
Queries sent:         73670
Queries completed:    73498 (99.77%)
Queries lost:         72 (0.10%)
Queries interrupted:  100 (0.14%)
Response codes:       NOERROR 73498 (100.00%)
Average packet size:  request 27, response 266  §
Run time (s):         453.044518
Queries per second:   162.231298
Average Latency (s):  0.610641 (min 0.021290, max 1.218650)
Latency StdDev (s):   0.049441
root@T460s:/home/muellega#
```

Content of input.csv

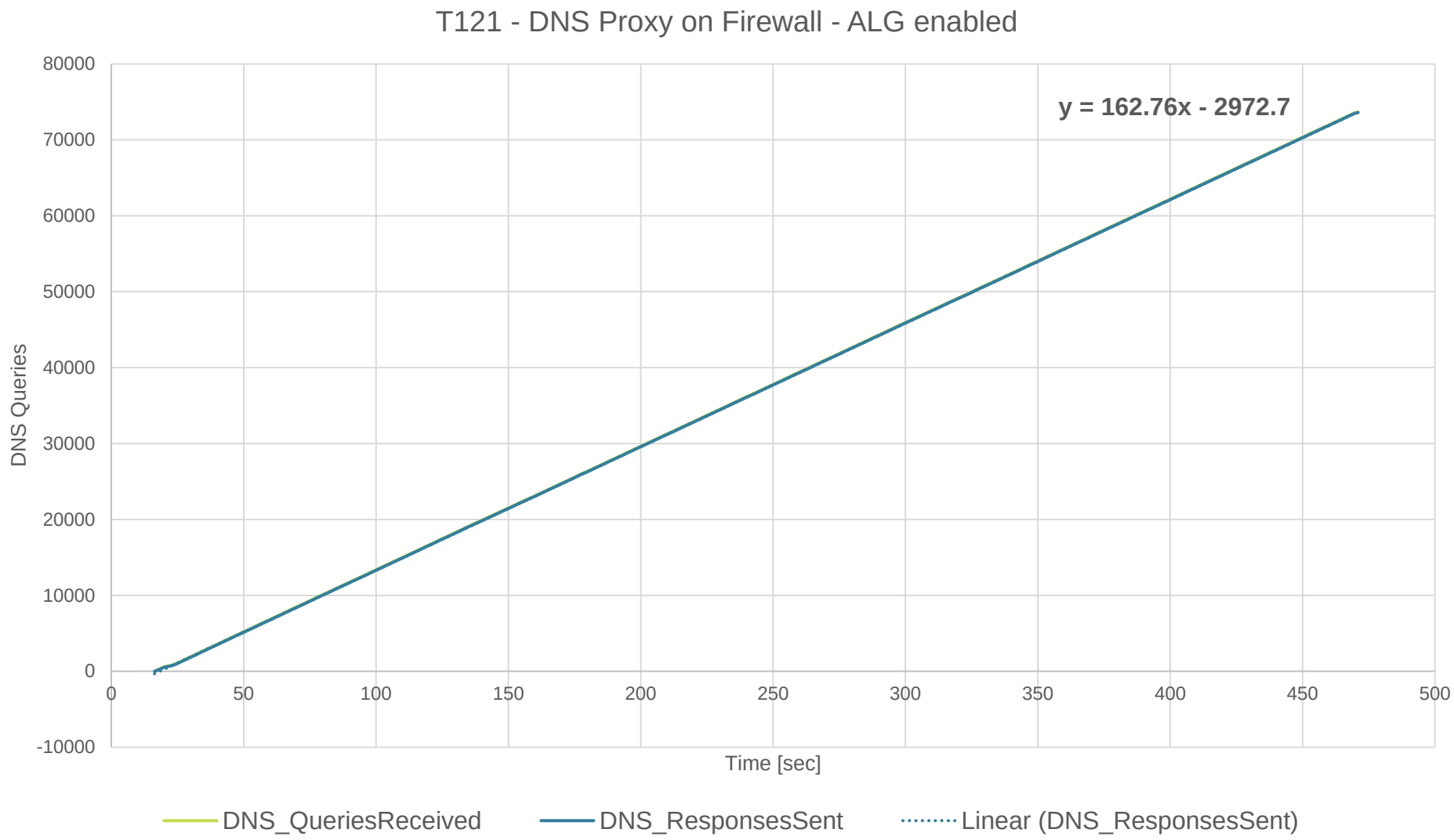
google.com AAAA

heise.de AAAA

T121 – DNS Proxy on Firewall – Load



T121 – DNS Proxy on Firewall – DNS Queries



T121 – DNS – Introduction to DNS ALG

Juniper DNS ALG Feature

- *DNS Application Layer Gateway (ALG) service provides an application layer gateway for use with DNS clients. DNS ALG service allows a client to access multiple DNS servers in different networks and provides routing to and from those servers. It also supports flexible address translation of the DNS query and response packets. These functions allow the DNS client to query many different domains from a single DNS server instance on the client side of the network.*

Disabling this feature

```
mug@srx210he2# set security alg dns disable
[edit]
mug@srx210he2# commit
commit complete
[edit]
mug@srx210he2#
```

T121 – DNS Proxy on Firewall – DNS ALG disabled

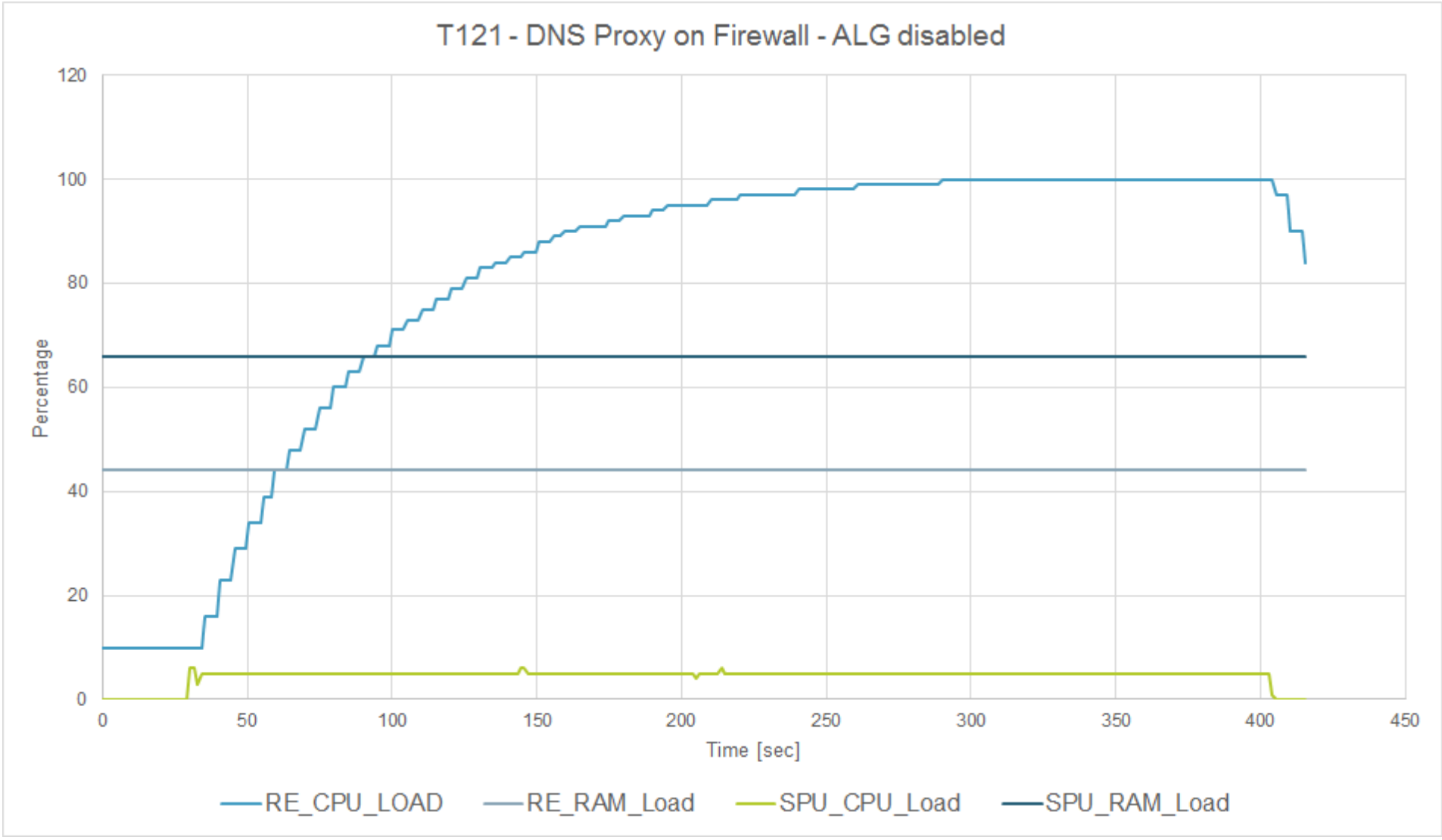
```
root@T460s:/home/muellega# ./dnsperf -s 2001:1702:6:20::1 -d input.tsv -l 600 -c 2000
DNS Performance Testing Tool Nominum Version 2.1.0.0
[Status] Command line: dnsperf -s 2001:1702:6:20::1 -d input.tsv -l 600 -c 2000
[Status] Sending queries (to 2001:1702:6:20::1)
[Status] Started at: Tue Feb 14 13:34:41 2017
[Status] Stopping after 600.000000 seconds...

Statistics:
Queries sent:         62217
Queries completed:    62078 (99.78%)
Queries lost:         39 (0.06%)
Queries interrupted:  100 (0.16%)
Response codes:       NOERROR 62078 (100.00%)
Average packet size:  request 27, response 265
Run time (s):         372.469636
Queries per second:   166.665935
Average Latency (s):  0.595919 (min 0.075896, max 0.769085)
Latency StdDev (s):   0.042583
root@T460s:/home/muellega#
```

Content of input.csv

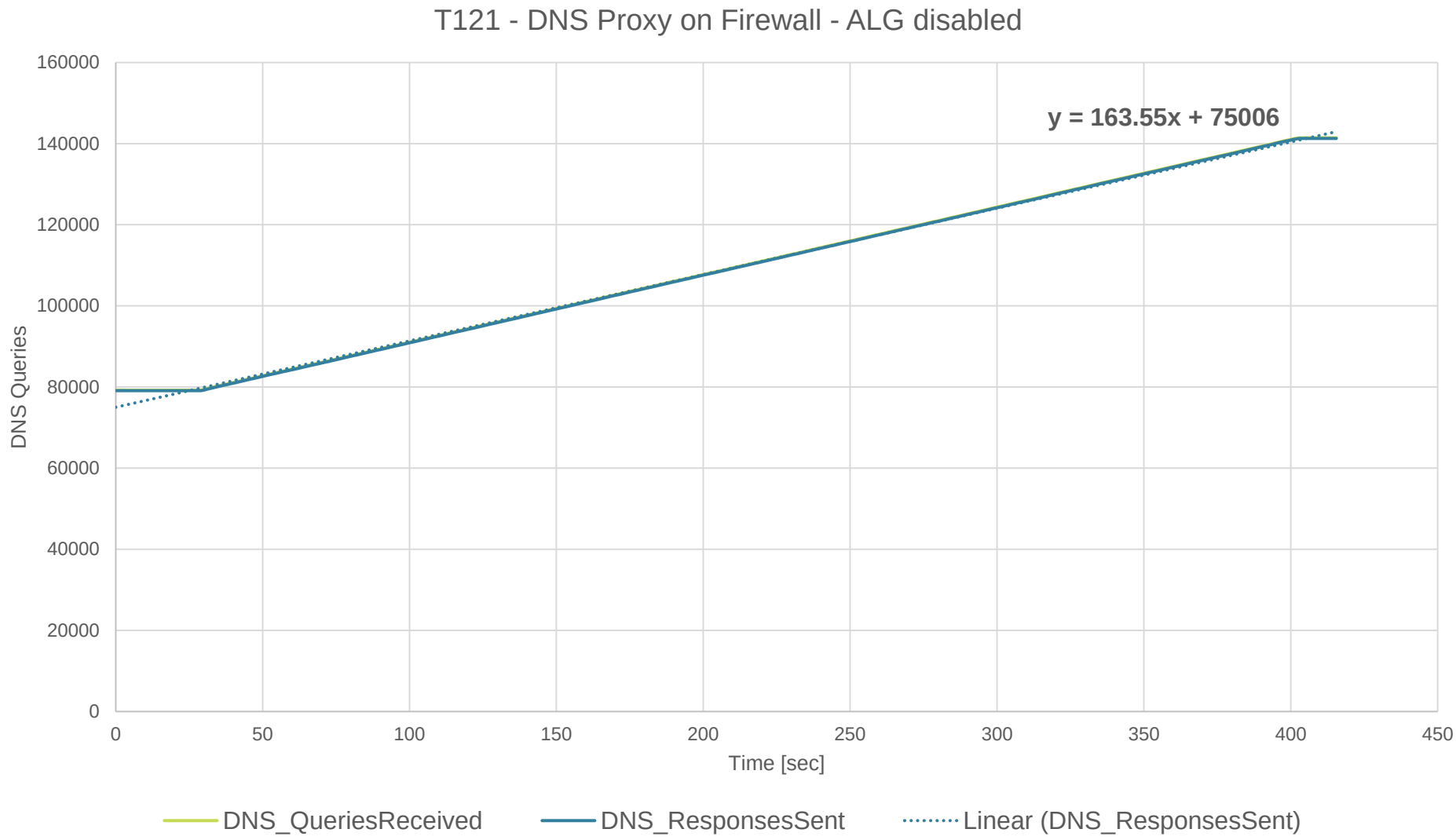
google.com AAAA

heise.de AAAA

T121 – DNS Proxy on Firewall – Load



T121 – DNS Proxy on Firewall – DNS Queries



T122 – DNS Server on HostB (over Firewall) – DNS ALG enabled

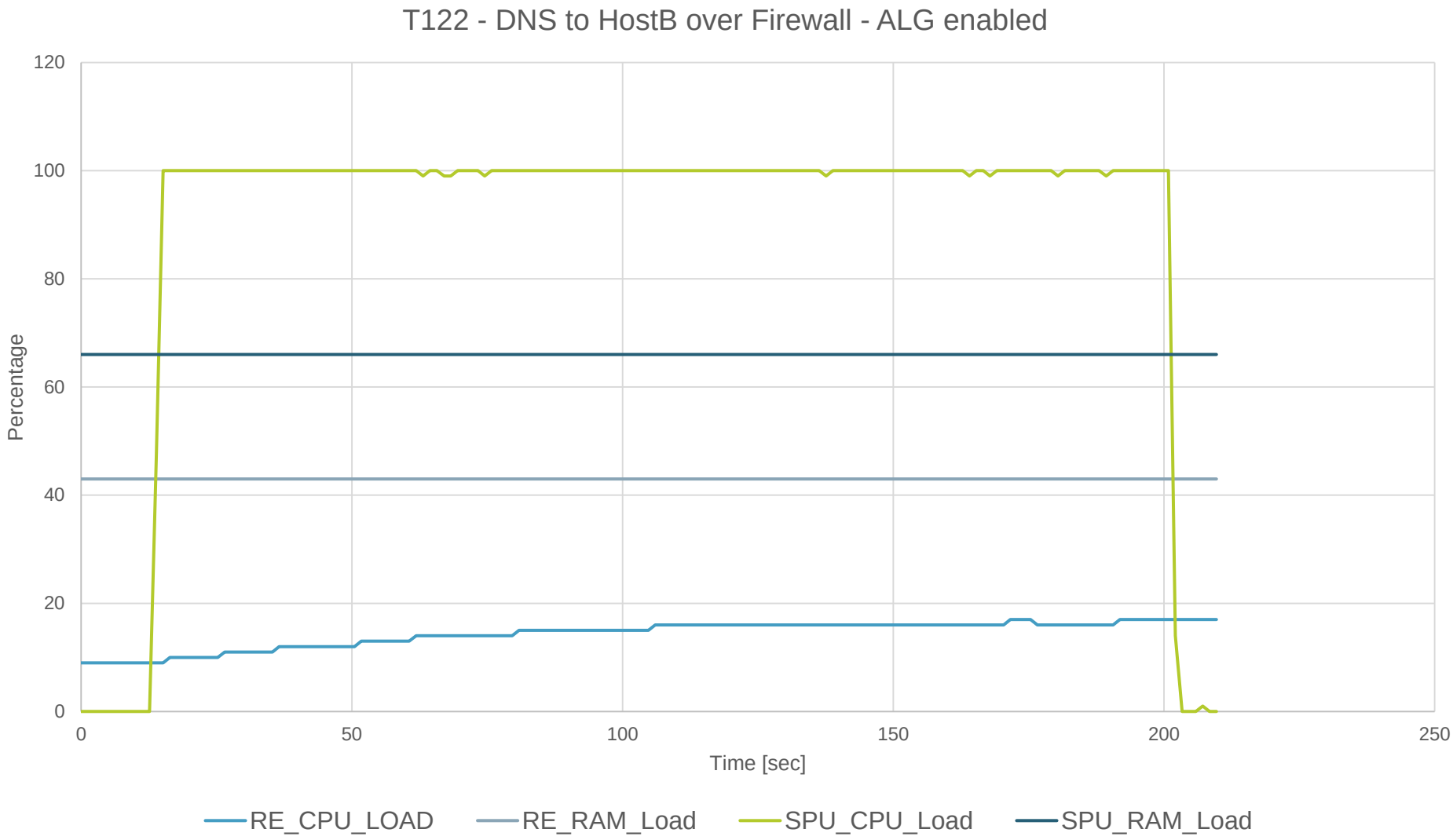
```
root@T460s:/home/muellega# ./dnsperf -s 2001:1702:6:10::10 -d input.tsv -l 600 -c
2000
DNS Performance Testing ToolNominum Version 2.1.0.0
[Status] Command line: dnsperf -s 2001:1702:6:10::10 -d input.tsv -l 600 -c 2000
[Status] Sending queries (to 2001:1702:6:10::10)
[Status] Started at: Tue Feb 14 13:15:46 2017
[Status] Stopping after 600.000000

Statistics:
Queries sent:         838636
Queries completed:    838542 (99.99%)
Queries lost:         0 (0.00%)
Queries interrupted:  94 (0.01%)
Response codes:       NOERROR 838542 (100.00%)
Average packet size:  request 27, response 55
Run time (s):         188.785130
Queries per second:   4441.779922
Average Latency (s):  0.022281 (min 0.000852, max 0.073489)
Latency StdDev (s):   0.001968
root@T460s:/home/muellega#
```

Content of input.csv

google.com AAAA

heise.de AAAA

T122 – DNS Server on HostB (over Firewall) – DNS ALG enabled – Load



T122 – DNS Server on HostB (over Firewall) – DNS ALG disabled

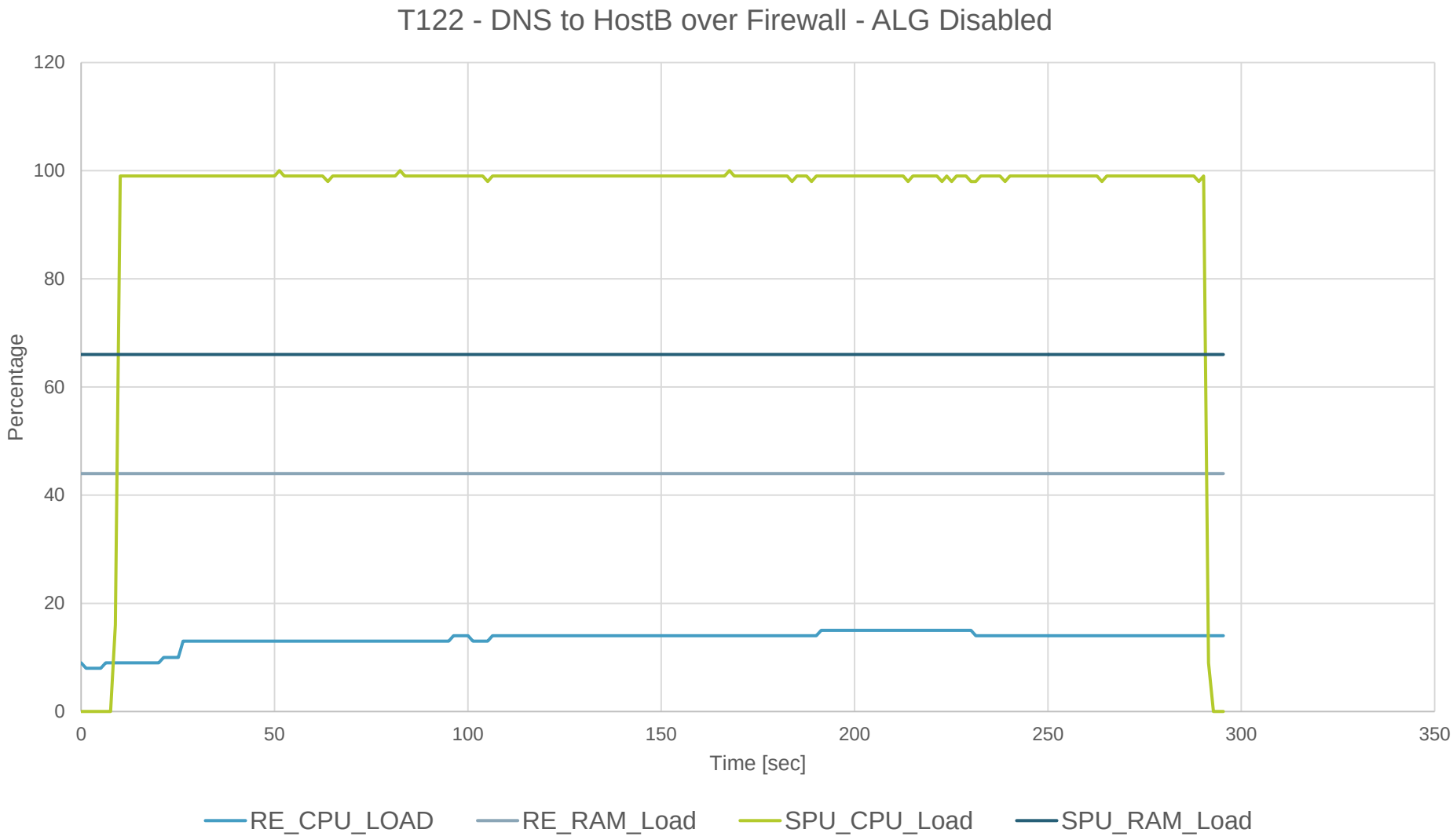
```
root@T460s:/home/muellega/# ./dnsperf -s 2001:1702:6:10::10 -d input.tsv -l 600 -c
2000
DNS Performance Testing ToolNominum Version 2.1.0.0
[Status] Command line: dnsperf -s 2001:1702:6:10::10 -d input.tsv -l 600 -c 2000
[Status] Sending queries (to 2001:1702:6:10::10)
[Status] Started at: Tue Feb 14 13:26:58 2017
[Status] Stopping after 600.000000

Statistics:
Queries sent:         9725792
Queries completed:    9725703 (100.00%)
Queries lost:         0 (0.00%)
Queries interrupted:  89 (0.00%)
Response codes:       NOERROR 9725703 (100.00%)
Average packet size:  request 27, response 55
Run time (s):         281.190865
Queries per second:   34587.549635
Average Latency (s):  0.002761 (min 0.000166, max 0.037740)
Latency StdDev (s):   0.000302
root@T460s:/home/muellega#
```

Content of input.csv

google.com AAAA

heise.de AAAA

T122 – DNS Server on HostB (over Firewall) – DNS ALG disabled – Load



T122 – DNS Server on HostB (direct)

```
root@T460s:/home/muellega# ./dnsperf -s 2001:1702:6:10::10 -d input.tsv -l 600 -c
2000
DNS Performance Testing Tool Nominum Version 2.1.0.0
[Status] Command line: dnsperf -s 2001:1702:6:10::10 -d input.tsv -l 600 -c 2000
[Status] Sending queries (to 2001:1702:6:10::10)
[Status] Started at: Tue Feb 14 15:36:47 2017
[Status] Stopping after 600.000000 seconds

Statistics:
Queries sent:         5606536
Queries completed:    5606436 (100.00%)
Queries lost:         0 (0.00%)
Queries interrupted:  100 (0.00%)
Response codes:       NOERROR 5606436 (100.00%)
Average packet size:  request 27, response 55
Run time (s):         114.105565
Queries per second:   49133.764861
Average Latency (s):  0.001942 (min 0.000374, max 0.019720)
Latency StdDev (s):   0.000283
root@T460s:/home/muellega#
```

Content of input.csv

google.com AAAA

heise.de AAAA

T12x – DNS – Summary

Performance

- SRX as DNS proxy
  - Fair (it is a branch firewall for small offices)
- SRX forwarding
  - Very good, if ALG is disabled

DNS ALG Feature

- We criticise default-on of the ALG DNS feature
- We had a déjà vu – our firewall migration beginning of 2016
  - *“To resolve the problems introduced by NAT, DNS ALG functionality has been extended to support static NAT and then the problems are resolved through DNS doctoring.”*

References DNS ALG

- https://www.juniper.net/techpubs/en_US/junos12.1/topics/concept/dns-alg-nat-doctoring-overview.html
- https://bart.motd.be/comment/2933

T13x – DHCPv6 – Short Recap

Table 8-1 DHCPv6 Message Types

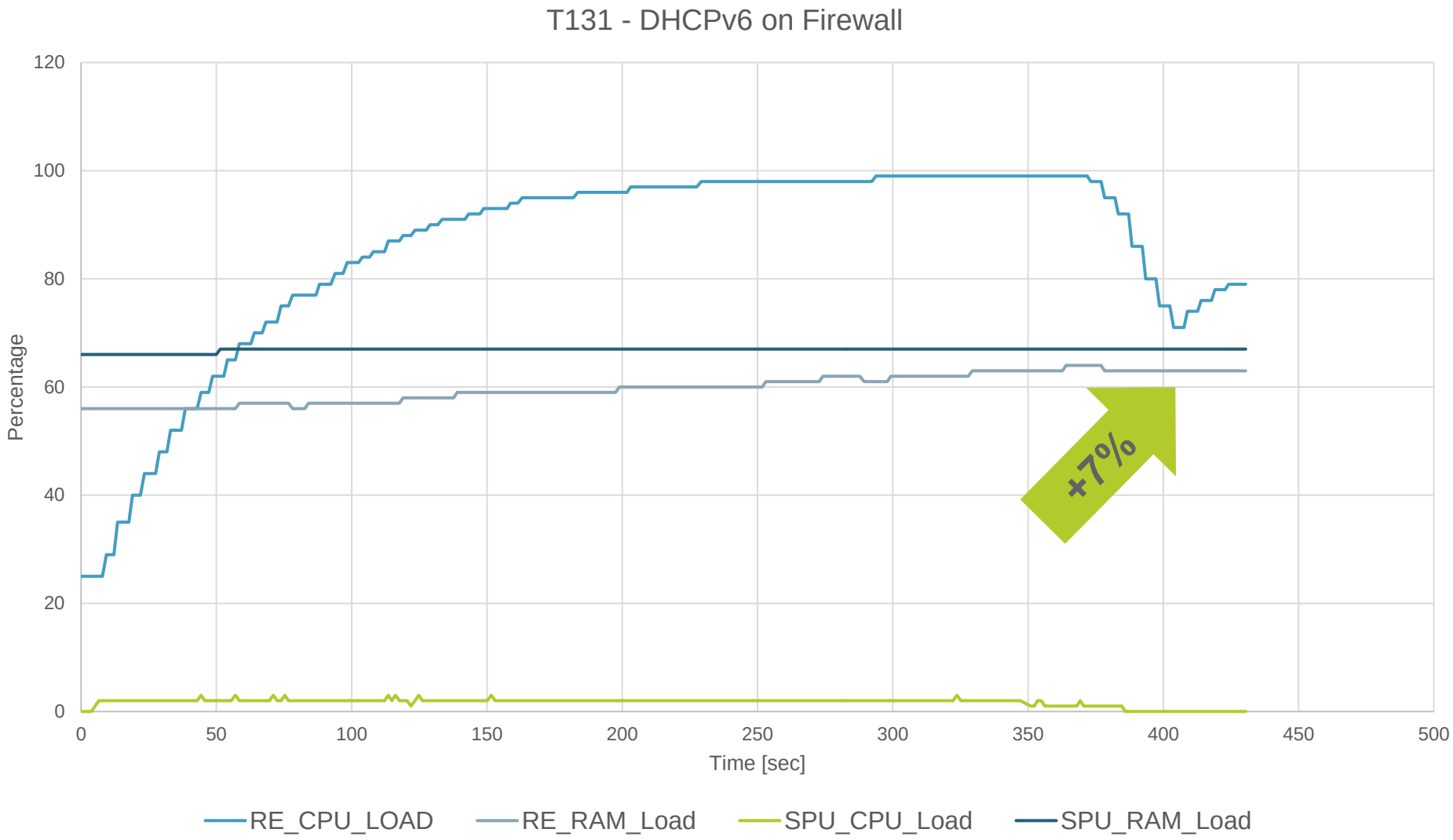
Msg-Type	Message	Description	Equivalent DHCP for IPv4 Message
1	Solicit	Sent by a client to locate servers.	DHCPDiscover
2	Advertise	Sent by a server in response to a Solicit message to indicate availability.	DHCPOffer
3	Request	Sent by a client to request addresses or configuration settings from a specific server.	DHCPRequest
7	Reply	Sent by a server to a specific client in response to a Solicit, Request, Renew, Rebind, Information-Request, Confirm, Release, or Decline message.	DHCPAck

Source: Microsoft Press – Understanding IPv6 2nd Edition

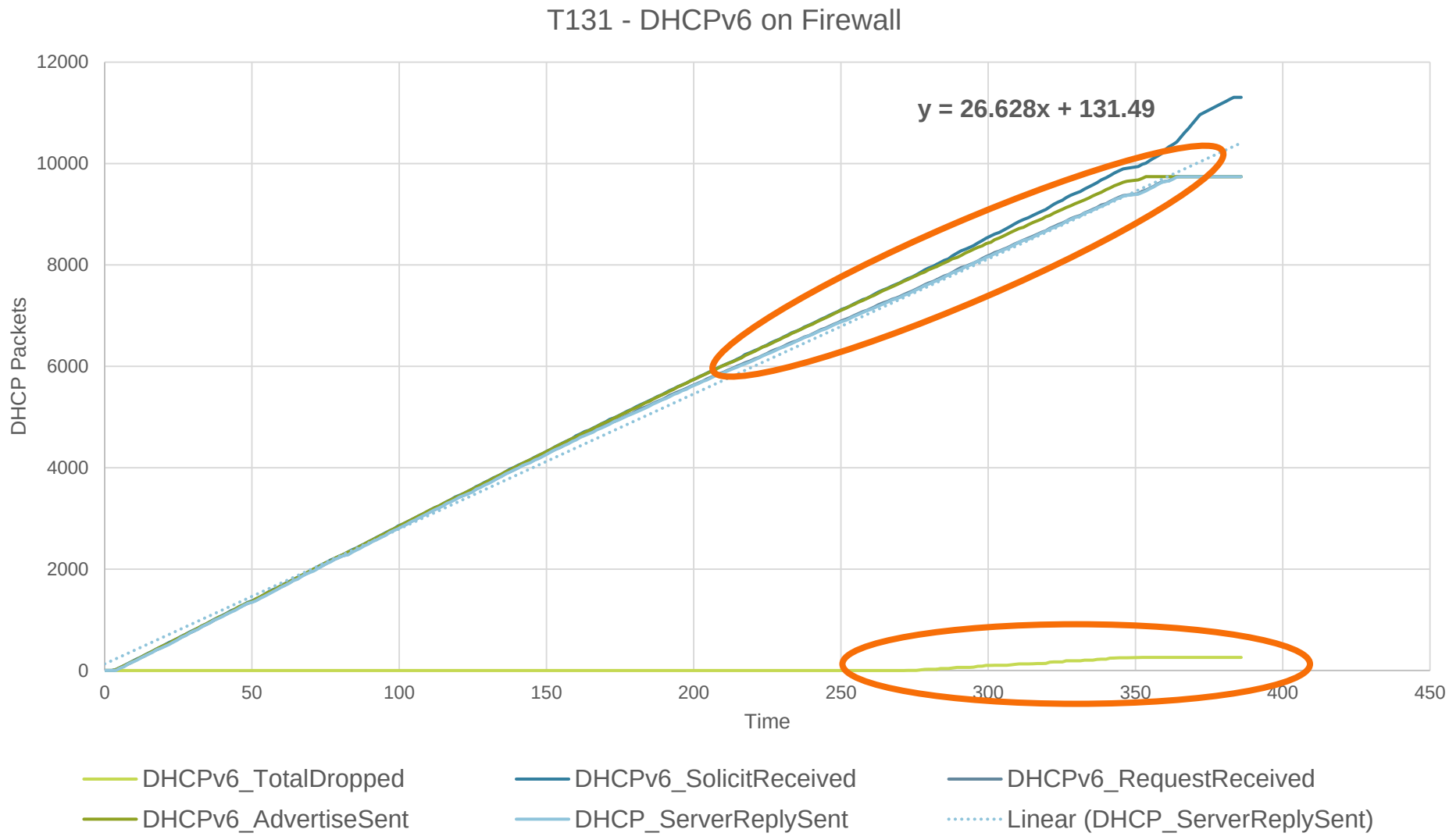
T131 – FW as DHCPv6 Server

```
Running: perfdhcp -6 -r 30 -R 10000 -l
Rate statistics
***Rate: 25.6523 exchanges/sec, expected rate: 30 exchanges/sec***
Statistics for:
 SOLICIT-ADVERTISE***
 sent packets: 9871
 received packets: 8535
 drops: 1336
 min/avg/max delay: 103.442 ms / 6550.926 ms / 8648.077 ms
 std deviation: 2195.988 ms
 collected packets: 0 // number of garbage collected packets

 REQUEST-REPLY***
 sent packets: 8535
 received packets: 8535
 drops: 0
 min/avg/max delay: 287.330 ms / 6727.545 ms / 8720.995 ms
 std deviation: 2135.060 ms
 collected packets: 0 // number of garbage collected packets

root@T460s:/home/muellega#
```

T131 – FW as DHCPv6 Server – Load



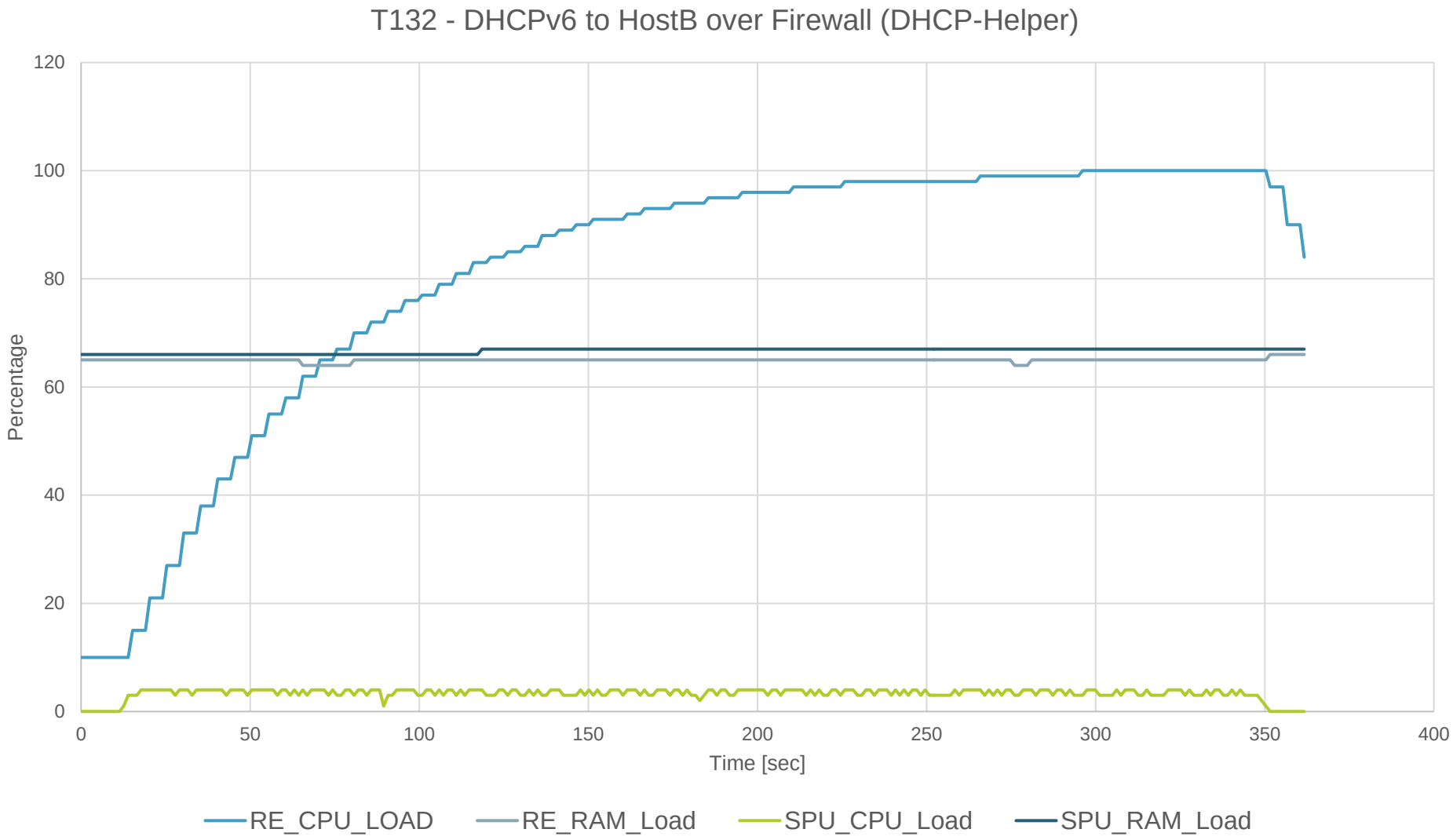
T131 – FW as DHCPv6 Server – DHCPv6 Requests



T132 – FW as DHCPv6 Relay

```
Running: perfdhcp -6 -r 30 -R 10000 -l
Rate statistics***
Rate: 25.6217 exchanges/sec, expected rate: 30 exchanges/sec***
Statistics for:
 SOLICIT-ADVERTISE***
 sent packets: 11305
 received packets: 9741
 drops: 1564
 min/avg/max delay: 89.660 ms / 4437.988 ms / 14170.165 ms
 std deviation: 3998.107 ms
 collected packets: 0 // number of garbage collected packets

 REQUEST-REPLY***
 sent packets: 9741
 received packets: 9741
 drops: 0
 min/avg/max delay: 272.248 ms / 4773.022 ms / 14263.719 ms
 std deviation: 4240.428 ms
 collected packets: 0 // number of garbage collected packets
root@T460s:/home/muellega#
```

T132 – FW as DHCPv6 Relay – Load



T133 – DHCPv6 Server on HostB (direct)

```
Running: perfdhcp -6 -r 200000 -R 100000 -l enp0s31f6
***Rate statistics***
Rate: 1869.74 exchanges/second, expected rate: 200000 exchanges/second
***Statistics for:
 SOLICIT-ADVERTISE***
 sent packets: 60661
 received packets: 60661
 drops: 0
 min/avg/max delay: 0.374 / 3.835 ms / 45.182 ms
 std deviation: 2.364 ms
 collected packets: 0 // number of garbage collected packets

 REQUEST-REPLY***
 sent packets: 60661
 received packets: 60661
 drops: 0
 min/avg/max delay: 1.627 ms / 6.275 ms/ 45.167 ms
 std deviation: 2.139 ms
 collected packets: 0 // number of garbage collected packets
root@T460s:/home/muellega#
```

T132 – FW as DHCPv6 Helper – pcap trace

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000…	2001:1702:6:20::1037	ff02::1:2	DHCPv6	114	Solicit XID: 0x0 CID: 000100012035cd9c000c01020304
2	0.2424…	2001:1702:6:20::1	2001:1702:6:20::1037	DHCPv6	184	Advertise XID: 0x0 CID: 000100012035cd9c000c01020304 IAA: 2001:1702:6:20::7335:2635
3	0.2465…	2001:1702:6:20::1037	ff02::1:2	DHCPv6	152	Request XID: 0x1 CID: 000100012035cd9c000c01020304 IAA: 2001:1702:6:20::7335:2635
4	0.6664…	2001:1702:6:20::1	2001:1702:6:20::1037	DHCPv6	179	Reply XID: 0x1 CID: 000100012035cd9c000c01020304 IAA: 2001:1702:6:20::7335:2635
5	1.0006…	2001:1702:6:20::1037	ff02::1:2	DHCPv6	114	Solicit XID: 0x2 CID: 000100012035cd9c000c01020305
6	1.2343…	2001:1702:6:20::1	2001:1702:6:20::1037	DHCPv6	184	Advertise XID: 0x2 CID: 000100012035cd9c000c01020305 IAA: 2001:1702:6:20::7335:2636
7	1.2363…	2001:1702:6:20::1037	ff02::1:2	DHCPv6	152	Request XID: 0x3 CID: 000100012035cd9c000c01020305 IAA: 2001:1702:6:20::7335:2636

```
    Hardware type: Ethernet (1)
    DUID Time: Jan 26, 2017 10:18:23.000000000 Mitteleurop?ische Zeit
    Link-layer address: 3c:97:0e:0e:50:38
  Identity Association for Non-temporary Address
    Option: Identity Association for Non-temporary Address (3)
    Length: 40
    Value: 0000000100000708000000c4e00050018200117020006002...
    IAID: 00000001
    T1: 1800
    T2: 3150
    IA Address
      Option: IA Address (5)
      Length: 24
      Value: 20011702000600200000000073352635000000e1000000e10
      IPv6 address: 2001:1702:6:20::7335:2635
      Preferred lifetime: 3600
      Valid lifetime: 3600
  Status code
    Option: Status code (13)
    Length: 9
    Value: 000073756363657373
    Status Code: Success (0)
    Status Message: success
  DNS recursive name server
    Option: DNS recursive name server (23)
    Length: 16
    Value: 20011702000600100000000000000010
     1 DNS server address: 2001:1702:6:10::10
```

T13x – DHCPv6 – Summary

Performance

- SRX as DHCPv6 Server
  - Fair (it is a branch firewall)
  - Limited in number of DHCPv6 states (about 5000 request)
- SRX as DHCPv6 Relay
  - Same performance – why (-:
- Interesting – stateless DHCPv6 performance
  - Why?

```
mug@srx210he2> show dhcpv6 server binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:1702:6:20::1037/128 56         1988     BOUND    ge-0/0/1.0   LL_TIME0x1…
2001:1702:6:20::1044/128 69         2125     BOUND    ge-0/0/1.0   LL_TIME0x1…
2001:1702:6:20::1045/128 70         2126     BOUND    ge-0/0/1.0   LL_TIME0x1…
…
```

  - How? → http://simkin.org/wordpress/?p=255

T13x – DHCPv6 – Summary – Router Advertisement

```
▼ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xb71c [correct]
    [Checksum Status: Good]
    Cur hop limit: 64
  ▼ Flags: 0x40
      0... .... = Managed address configuration: Not set
      .1.. .... = Other configuration: Set
      ..0. .... = Home Agent: Not set
      ...0 0... = Prf (Default Router Preference): Medium (0)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ▸ ICMPv6 Option (Source link-layer address : 10:0e:7e:d3:ab:01)
  ▼ ICMPv6 Option (Prefix information : 2001:1702:6:20::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    ▼ Flag: 0xc0
        1... .... = On-link flag(L): Set
        .1.. .... = Autonomous address-configuration flag(A): Set
        ..0. .... = Router address flag(R): Not set
        ...0 0000 = Reserved: 0
      Valid Lifetime: 2592000
      Preferred Lifetime: 604800
      Reserved
      Prefix: 2001:1702:6:20::
```

T13x – DHCPv6 – Summary – DHCPv6 Reply (to Information Request)

```
1… 18.3565… fe80::20:0:0:1                fe80::ac9b:c54f:29f9:3a3e    DHC… 154 Reply XID: 0xa68b15 CID: 000100012013dbc8001122334455
▸ Frame 199: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0
▸ Ethernet II, Src: JuniperN_d3:ab:01 (10:0e:7e:d3:ab:01), Dst: LcfcHefe_64:c8:88 (c8:5b:76:64:c8:88)
▸ Internet Protocol Version 6, Src: fe80::20:0:0:1, Dst: fe80::ac9b:c54f:29f9:3a3e
▸ User Datagram Protocol, Src Port: 547, Dst Port: 546
DHCPv6
  Message type: Reply (7)
  Transaction ID: 0xa68b15
  ▾ Client Identifier
    Option: Client Identifier (1)
    Length: 14
    Value: 000100012013dbc8001122334455
    DUID: 000100012013dbc8001122334455
    DUID Type: link-layer address plus time (1)
    Hardware type: Ethernet (1)
    DUID Time: Jan 19, 2017 21:19:20.000000000 CET
    Link-layer address: 00:11:22:33:44:55
  ▾ Server Identifier
    Option: Server Identifier (2)
    Length: 26
    Value: 00020000058343443530313341 4b31343936000000000000...
    DUID: 00020000058343443530313341 4b31343936000000000000...
    DUID Type: assigned by vendor based on Enterprise number (2)
    Enterprise ID: Juniper Networks/Funk Software (1411)
    Identifier: 434435303133414b3134393600000000000000000
  ▾ DNS recursive name server
    Option: DNS recursive name server (23)
    Length: 16
    Value: 20011702000600200000000000000001
     1 DNS server address: 2001:1702:6:20::1
  ▾ DNS recursive name server
    Option: DNS recursive name server (23)
    Length: 16
    Value: 20011702000600200000000000000001
     1 DNS server address: 2001:1702:6:20::1
```

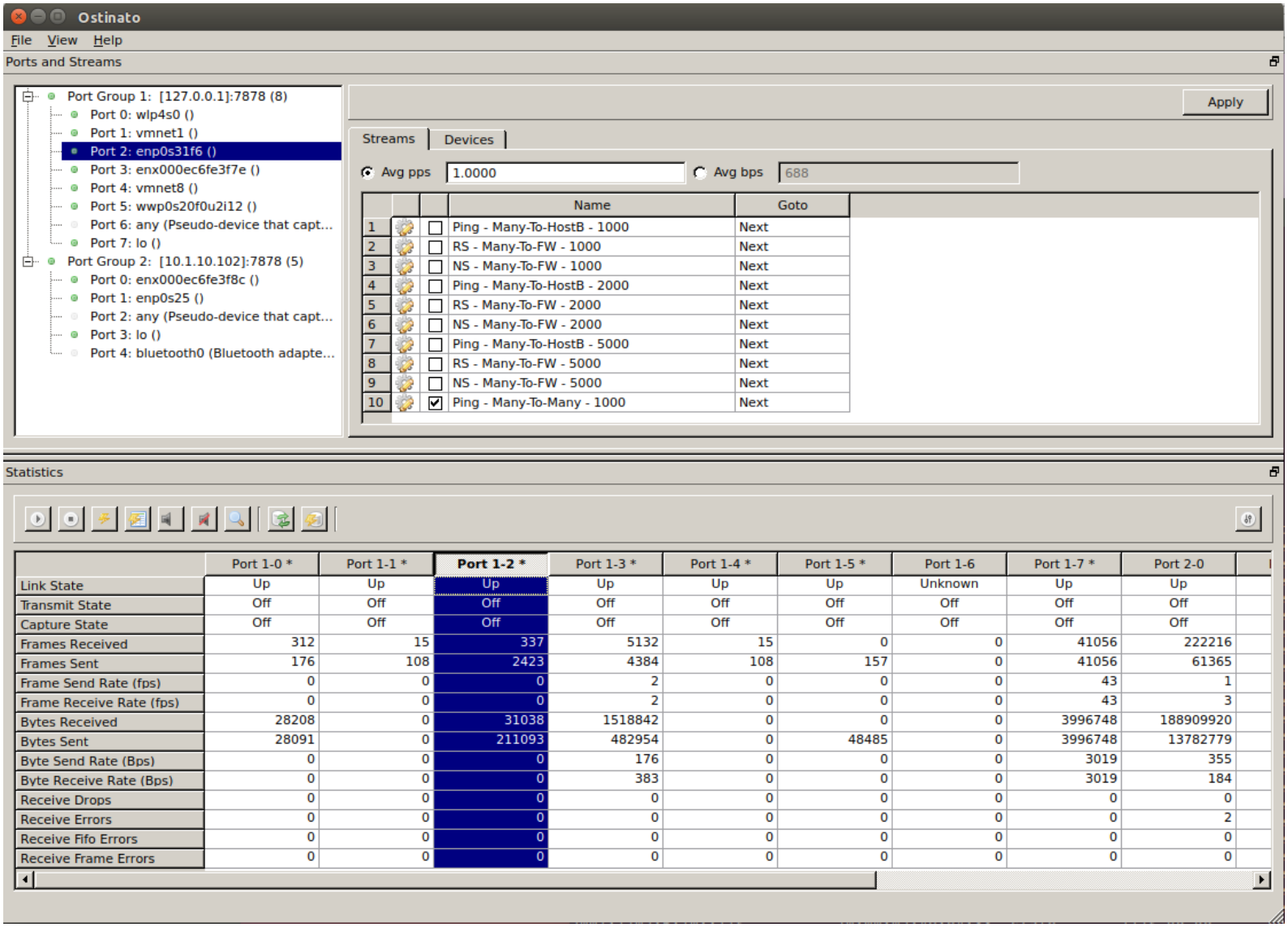
```
mug@srx210he2> show dhcpv6 server binding

mug@srx210he2>
```

Contents

Test Case Overview

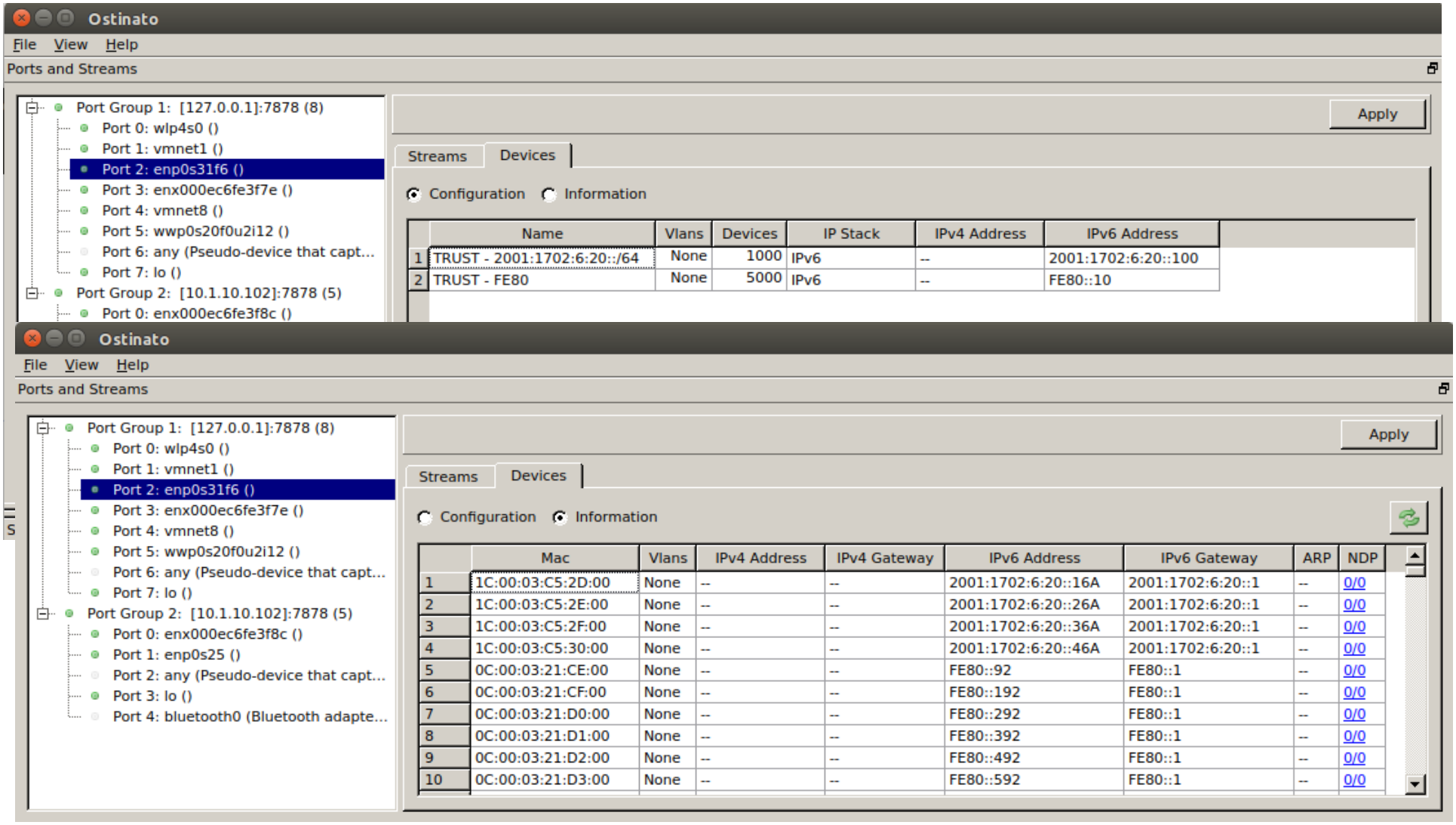
- T201: Router Solicitation Messages to Firewall
- T211: Neighbor Solicitation Messages to Firewall
- T221: Send ICMP Echo Requests to Network of HostB over Firewall

Introduction Ostinato – GUI



	Port 1-0 *	Port 1-1 *	Port 1-2 *	Port 1-3 *	Port 1-4 *	Port 1-5 *	Port 1-6	Port 1-7 *	Port 2-0
Link State	Up	Up	Up	Up	Up	Up	Unknown	Up	Up
Transmit State	Off	Off	Off	Off	Off	Off	Off	Off	Off
Capture State	Off	Off	Off	Off	Off	Off	Off	Off	Off
Frames Received	312	15	337	5132	15	0	0	41056	222216
Frames Sent	176	108	2423	4384	108	157	0	41056	61365
Frame Send Rate (fps)	0	0	0	2	0	0	0	43	1
Frame Receive Rate (fps)	0	0	0	2	0	0	0	43	3
Bytes Received	28208	0	31038	1518842	0	0	0	3996748	188909920
Bytes Sent	28091	0	211093	482954	0	48485	0	3996748	13782779
Byte Send Rate (Bps)	0	0	0	176	0	0	0	3019	355
Byte Receive Rate (Bps)	0	0	0	383	0	0	0	3019	184
Receive Drops	0	0	0	0	0	0	0	0	0
Receive Errors	0	0	0	0	0	0	0	0	2
Receive Fifo Errors	0	0	0	0	0	0	0	0	0
Receive Frame Errors	0	0	0	0	0	0	0	0	0

Introduction Ostinato – GUI



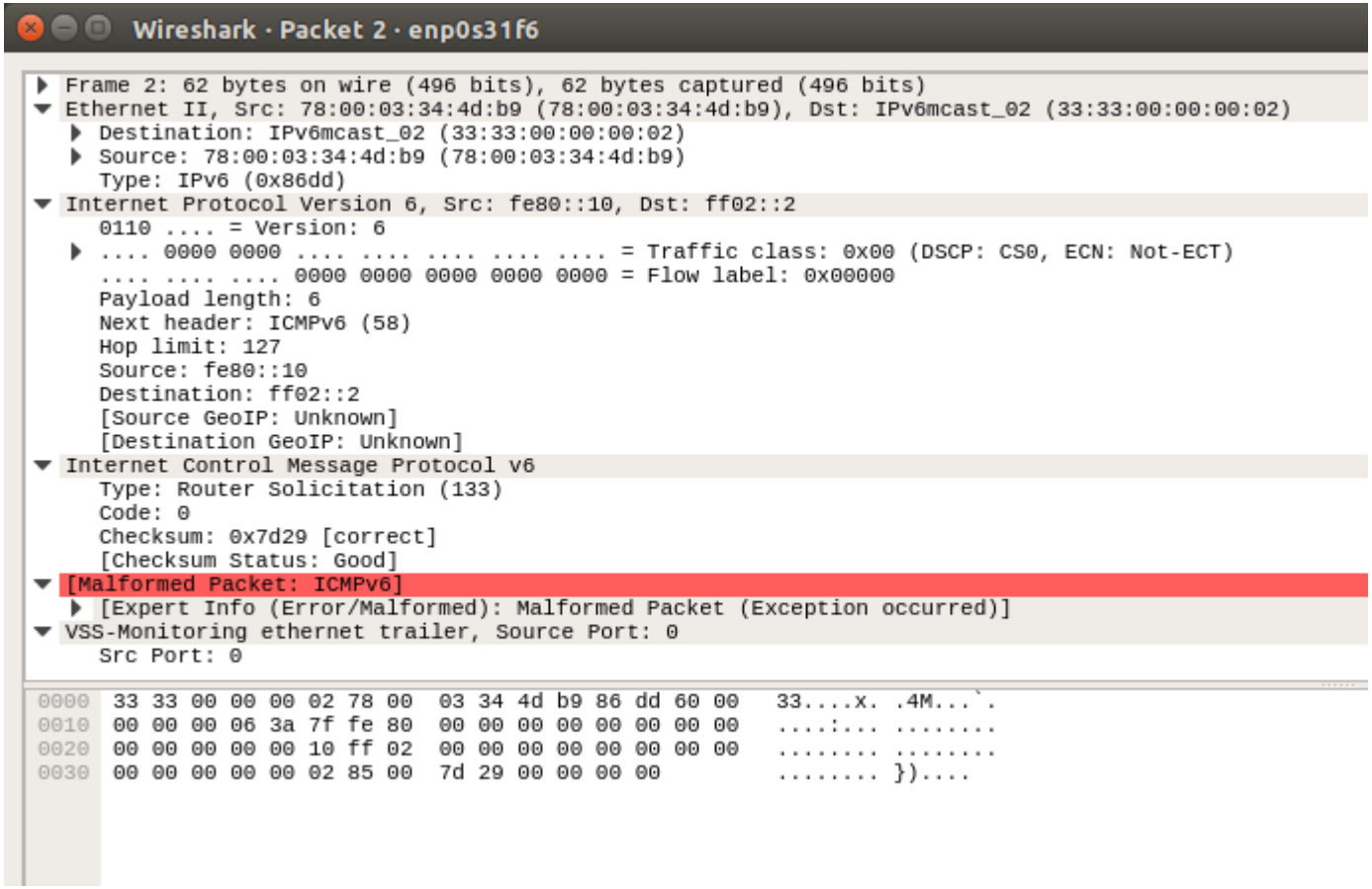
Introduction Ostinato – Crafting a Packet

Router Solicitation Packet

- MAC
  - Src: MAC of sending network adapter
  - Dst: 33:33:00:00:00:02
- IPv6
  - Src: Link local address of sending network adapter (or ::)
  - Dst: FF02::2
  - Hop Limit: 255
- ICMPv6
  - Type: 133
  - Code: 0
  - Checksum: ICMPv6 checksum
  - Reserved: 32bit field – future use – set to 0

Introduction Ostinato – Crafting a Packet – 1st Try

Router Solicitation Packet



Introduction Ostinato – Crafting a Packet – 2nd Try

Router Solicitation Packet

Wireshark · Packet 13 · wireshark_enp0s31f6_20170116224254_hwCye1

```
▼ Frame 13: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
    Interface id: 0 (enp0s31f6)
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan 16, 2017 22:43:09.198124811 CET
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1484602989.198124811 seconds
    [Time delta from previous captured frame: 1.000000080 seconds]
    [Time delta from previous displayed frame: 1.000000080 seconds]
    [Time since reference or first frame: 8.999988661 seconds]
    Frame Number: 13
    Frame Length: 62 bytes (496 bits)
    Capture Length: 62 bytes (496 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
▼ Ethernet II, Src: 78:00:03:34:4d:b9 (78:00:03:34:4d:b9), Dst: IPv6mcast_02 (33:33:00:00:00:02)
  ▶ Destination: IPv6mcast_02 (33:33:00:00:00:02)
  ▶ Source: 78:00:03:34:4d:b9 (78:00:03:34:4d:b9)
    Type: IPv6 (0x86dd)
▼ Internet Protocol Version 6, Src: fe80::10, Dst: ff02::2
    0110 .... = Version: 6
  ▶ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000
    Payload length: 8
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::10
    Destination: ff02::2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0x7d27 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
```

T201 – Router Solicitation Messages to Firewall

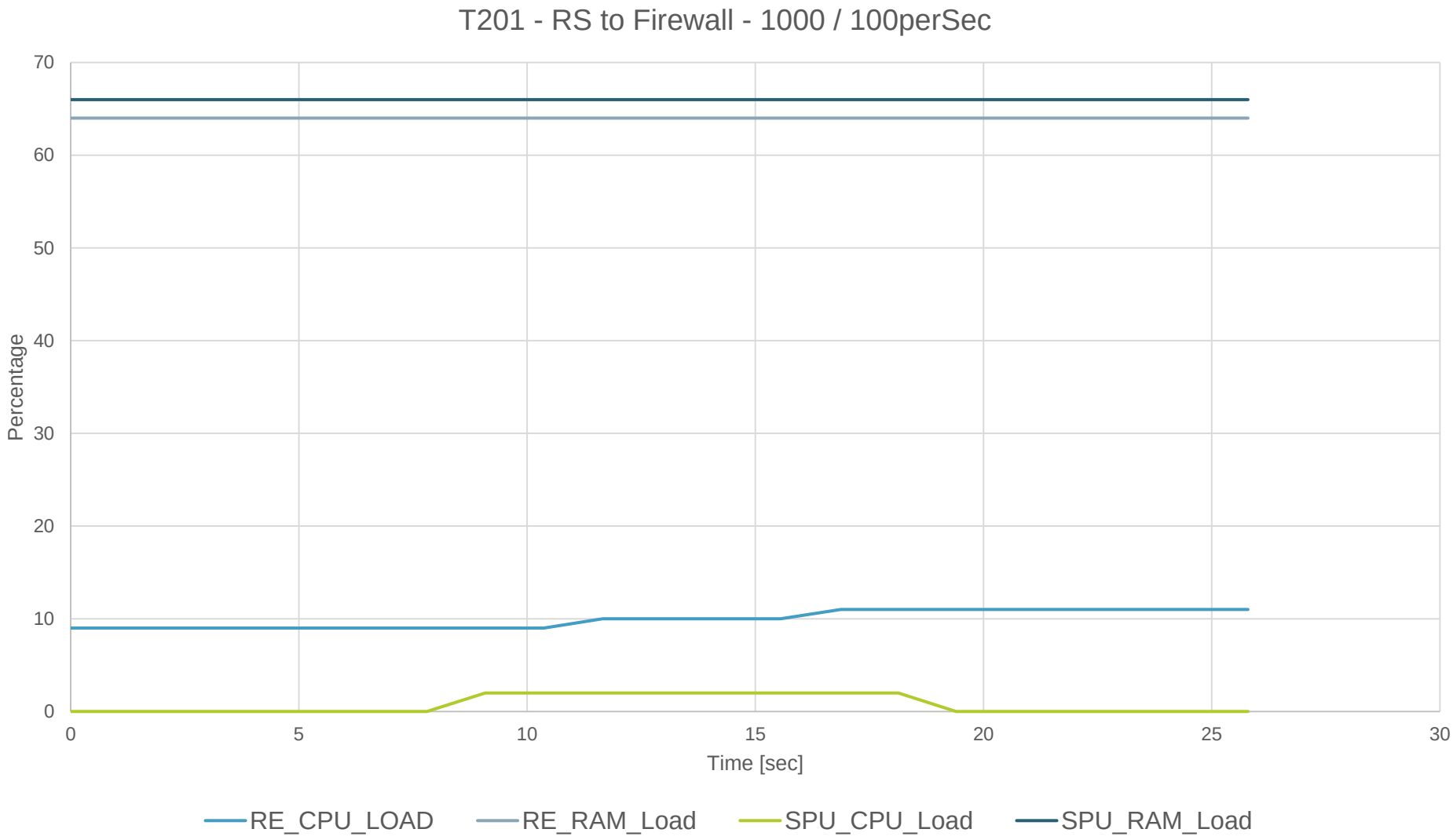
Number of RS and Send Rate

- T201a: 1000 RS / 100 per second
- T201b: 1000 RS / 200 per second
- T201c: 10000 RS / 500 per second

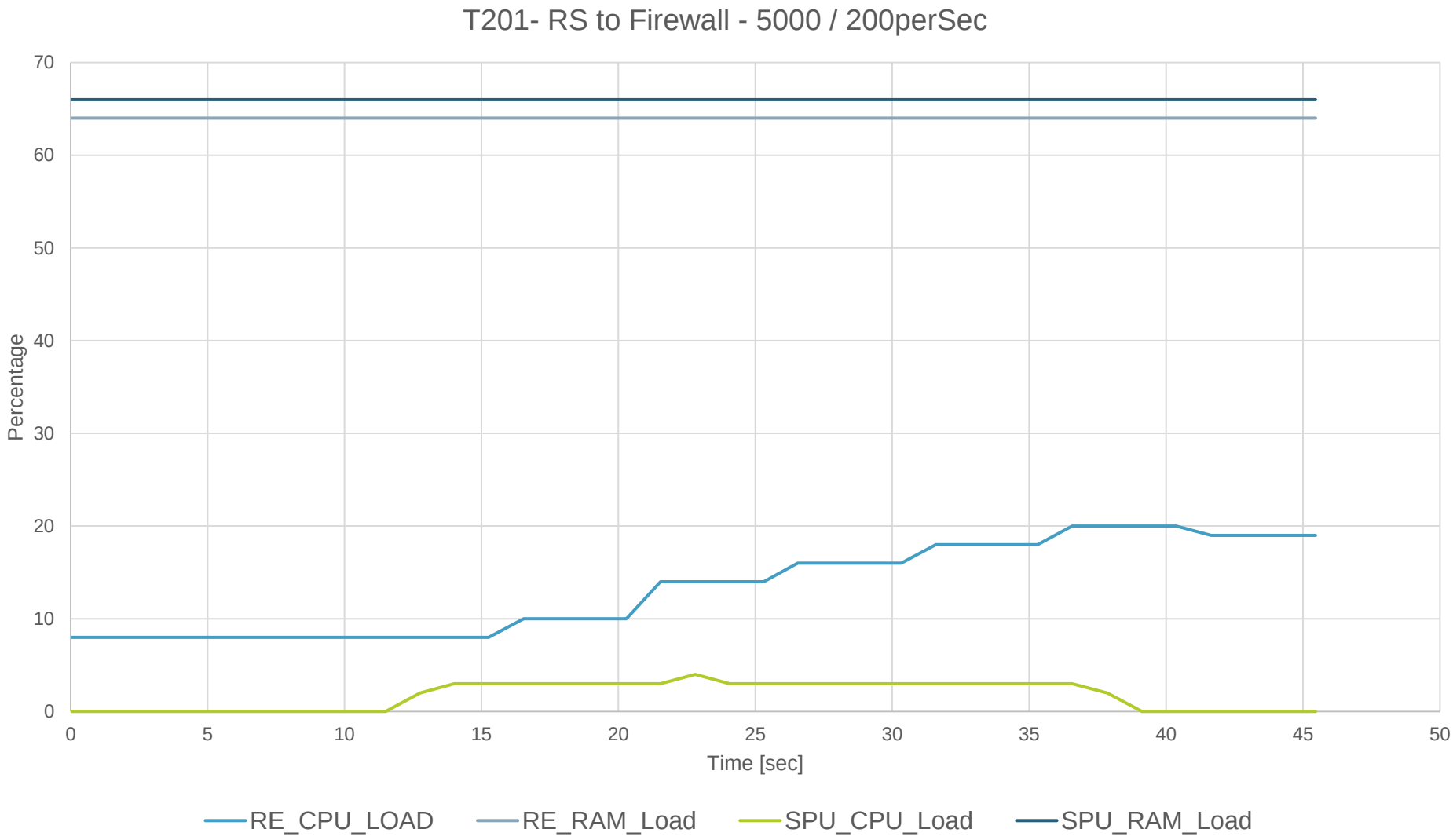
What do we expect ?

- Traffic destinated to control plane
  - Hence high CPU load on RE

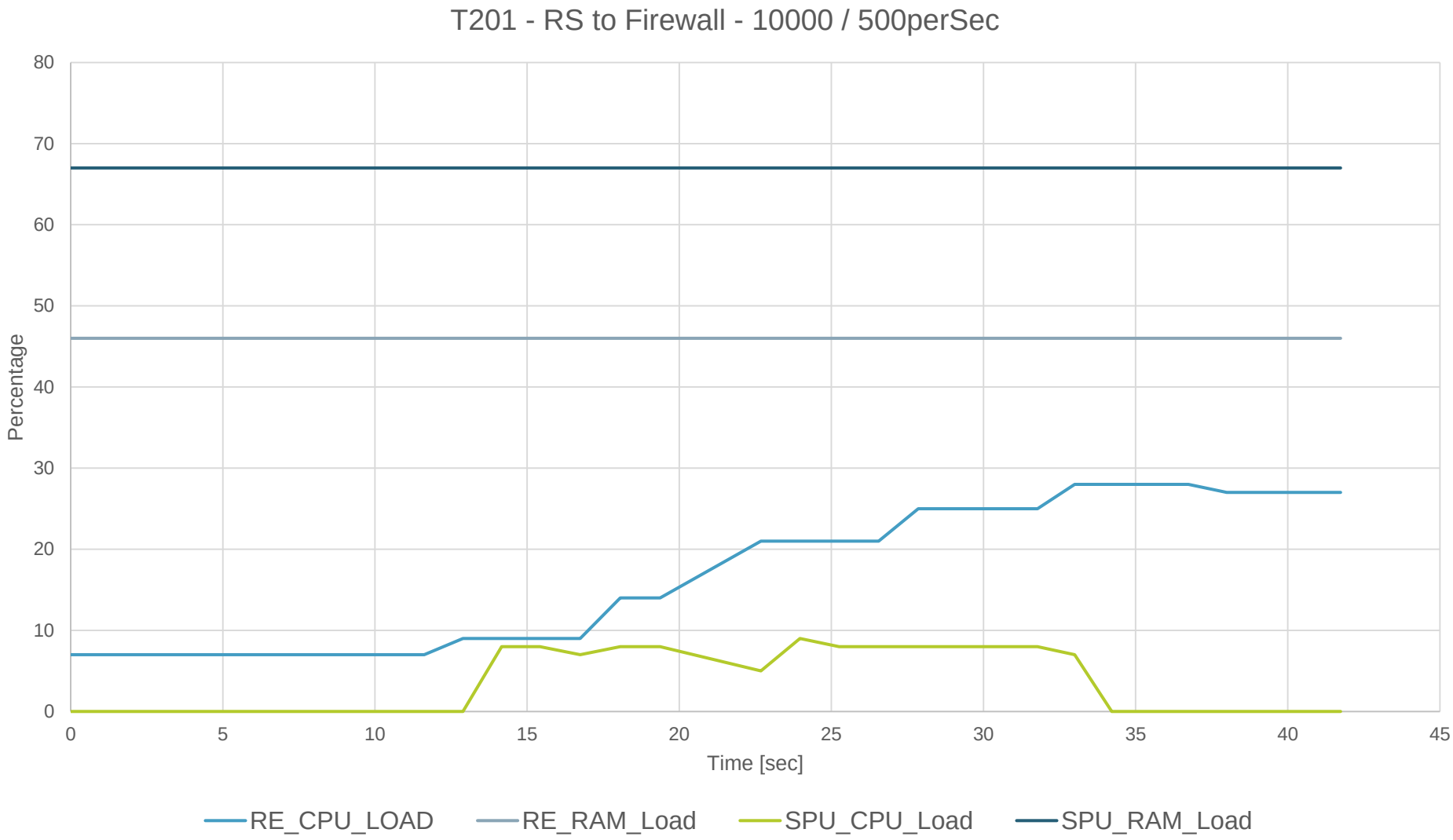
T201a – Router Solicitation Messages to Firewall – Load



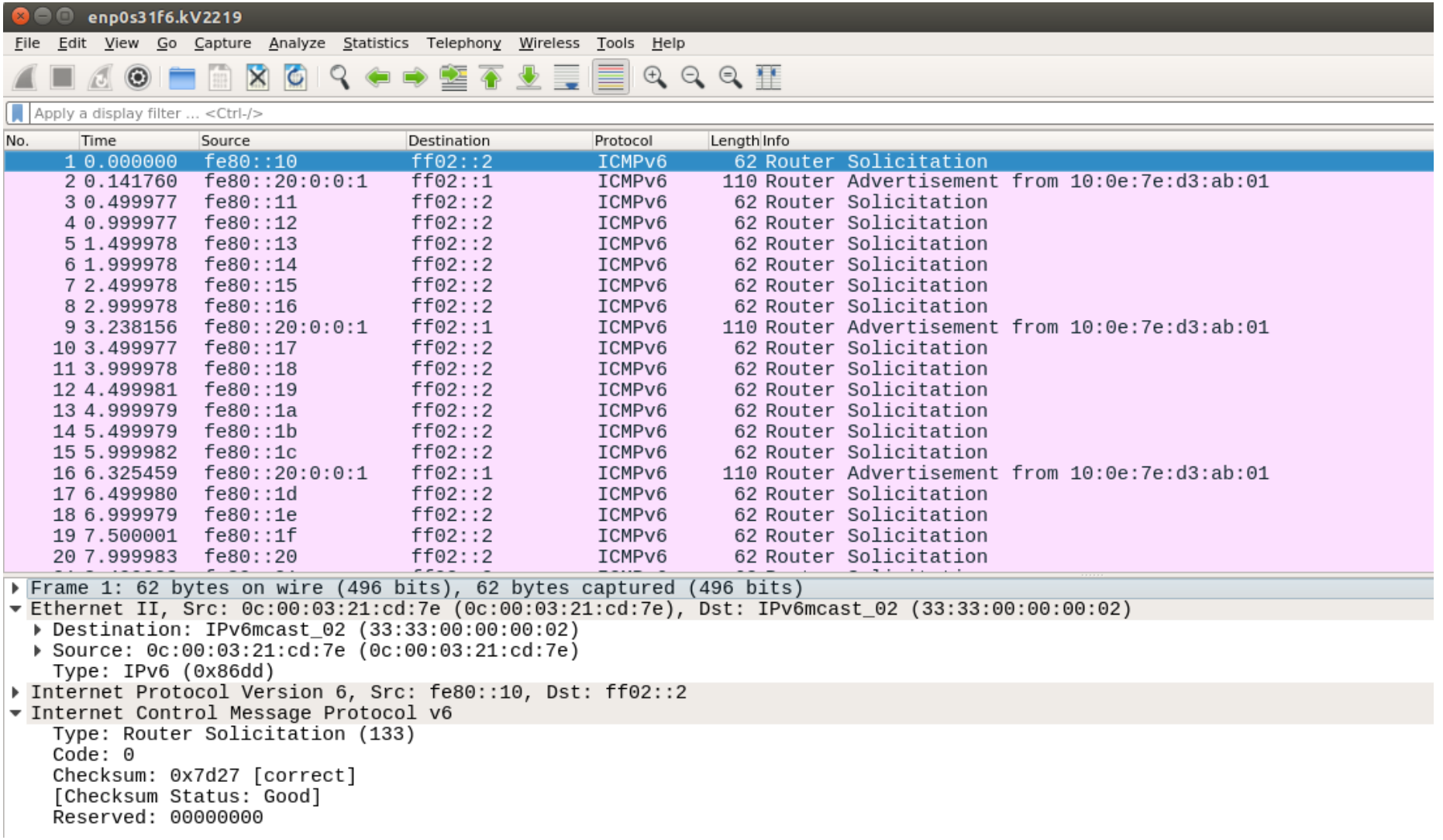
T201b – Router Solicitation Messages to Firewall – Load



T201c – Router Solicitation Messages to Firewall – Load



T201 – Interesting Observation



T201 – Router Solicitation Messages to Firewall – Summary

Performance

- Good performance
  - Supports recommendation to use stateless address configuration
- SRX Response to RS
  - Not sending a response for each RS
  - For us valid approach due the fact RA is addressed to all nodes (FF02::1)

T211 – Neighbour Solicitation Messages to Firewall

Number of RS and Send Rate

- T211a: 1000 NS / 20 per second
- T211b: 2000 NS / 50 per second

What do we expect?

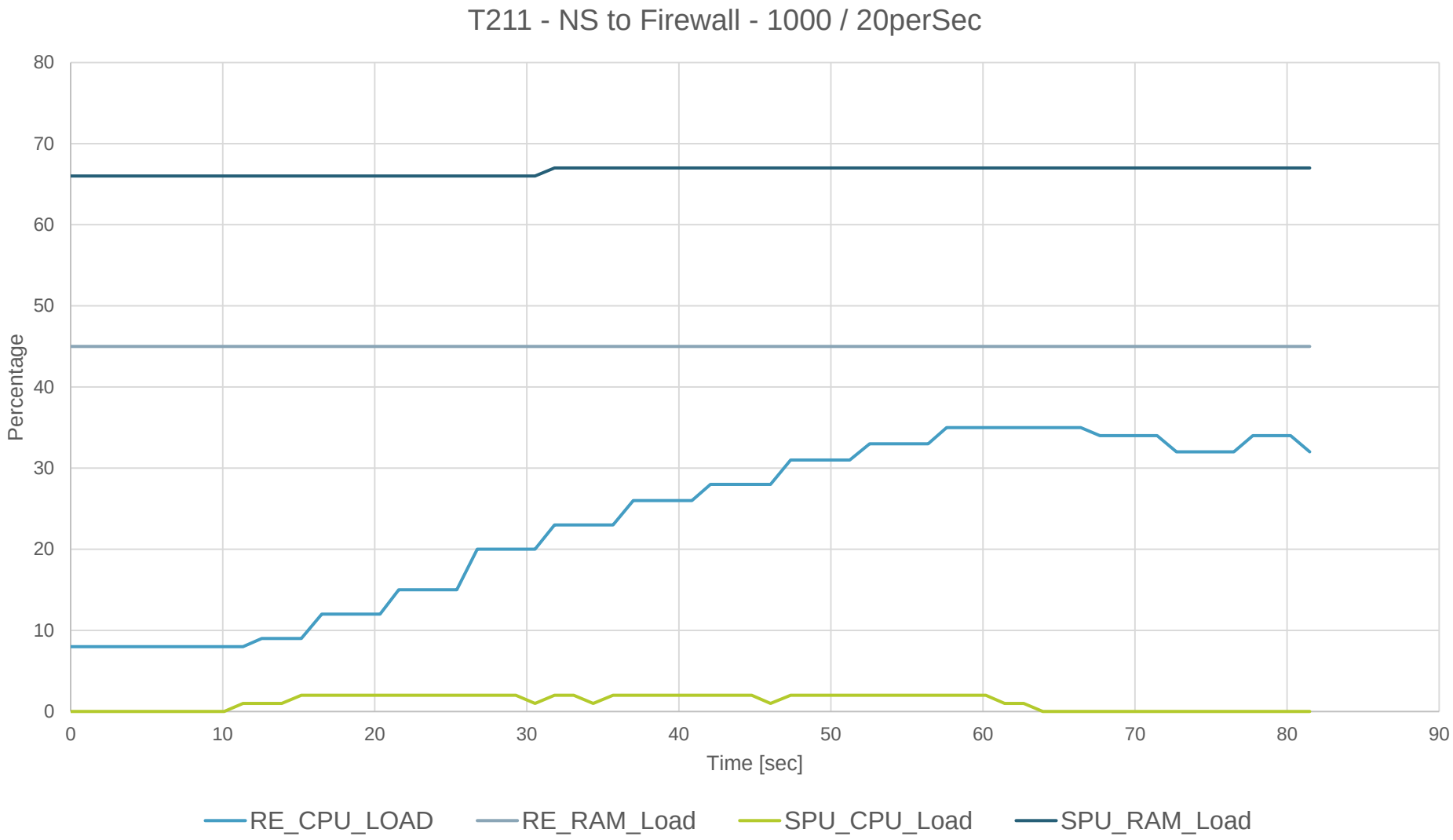
- Traffic destinated to control plane
  - Hence high CPU load on RE
  - Since unicast NS, firewall has to respond to each NS request,
    - Hence, higher CPU load of control plane (compared to RS messages)

T211 – Neighbour Solicitation Messages to Firewall – Crafting the Packet

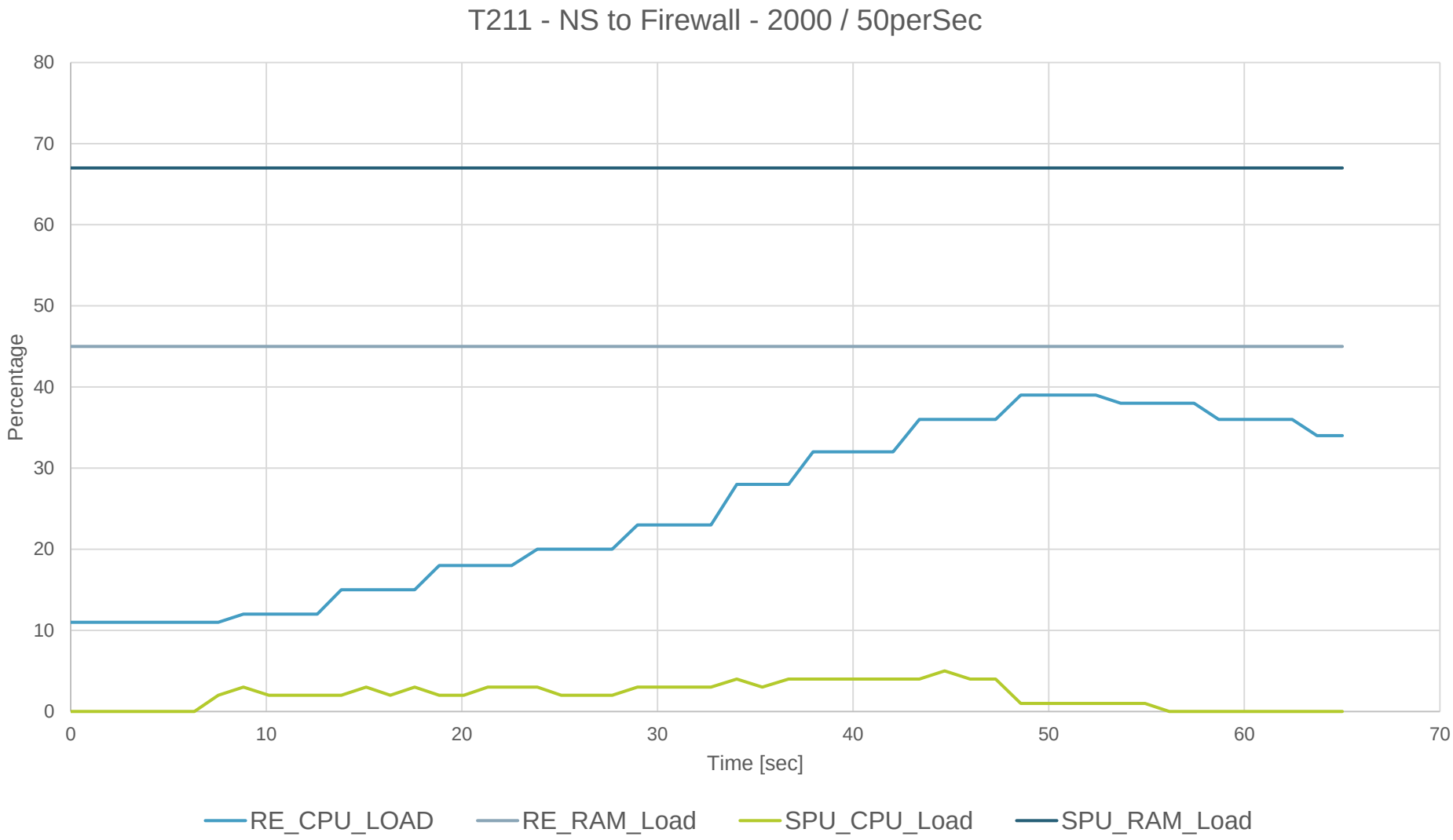
Unicast Neighbour Solicitation Message

- MAC
  - Src: MAC of sending network adapter
  - Dst: MAC of firewall interface
- IPv6
  - Src: Link local address of sending network adapter
  - Dst: Link local address of firewall interface
  - Hop Limit: 255
- ICMPv6
  - Type: 135
  - Code: 0
  - Checksum: ICMPv6 checksum
  - Reserved: 32bit field – future use – set to 0
  - Payload: Link local address of firewall: fe80:0000:0000:0000:0020:0000:0000:00001

T211a – Neighbor Solicitation Messages to Firewall – Load



T211b – Neighbor Solicitation Messages to Firewall – Load



T211 – Neighbour Solicitation Messages to Firewall – Summary

Performance

- Fair, but given the below, acceptable

Load

- Significantly higher compared to RS messages
  - Unicast NS requires response to each request
  - In addition, firewall is required to read / process payload information

T221 – Send ICMP Echo Requests to Network of HostB over Firewall

Motivation

- Firewall has to route packets from TRUST to UNTRUST zone
- In addition, firewall has to determine MAC addresses
  - Has to send NS messages in case address is not in neighbour cache

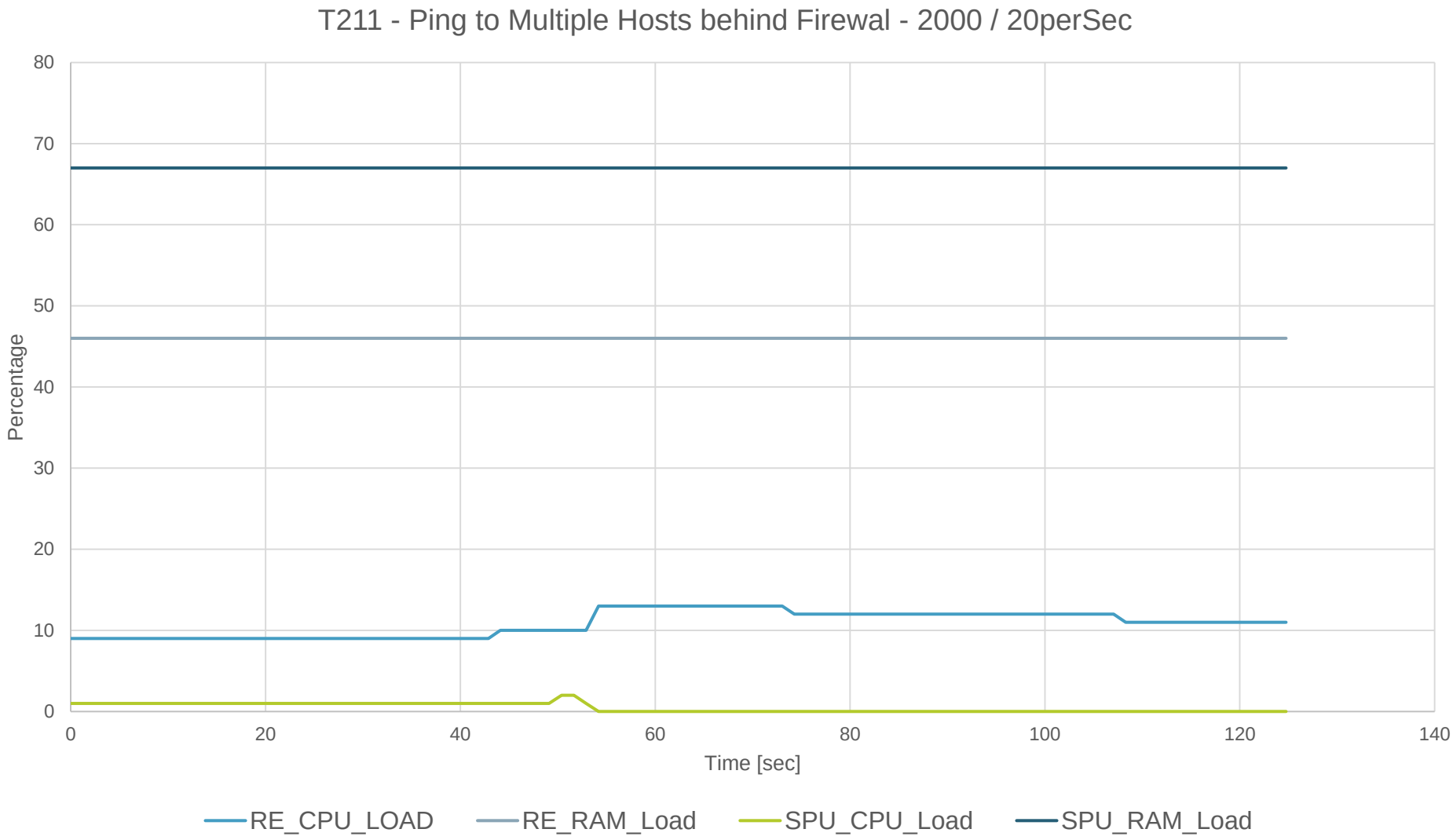
To do

- Crafting ICMP echo request packets
- Simulate target nodes (Ostinato has to respond to NS messages of firewall)

What do we expect

- Depends
  - If MAC already in neighbour cache → fast (data plane / SPU)
  - If not → higher load of control plane / RE due to required NS message and update of cache

T221 – Send ICMP Echo Requests to Network of HostB over Firewall – Load



T221 – Send ICMP Echo Requests to Network of HostB over Firewall – Summary

Performance

- Good with the simulated load (20 echo requests per second)

Comments

- Higher loads not possible due to unstable Ostinato
- Ostinato did not send echo responses back → load on firewall is lower than in real world scenario

Contents

Summarized

Device under Test (DuT) – SRX210HE2

- Considering its targeted usage (branch office): Very good
  - Especially: Could never exhaust memory
- To consider: Very basic configuration
  - Network level - no dynamic routing, not IPSec, no syslog…
  - Application – no AV

Testing itself

- Simulating traffic / nodes challenging
  - Requires detailed protocol knowledge
  - Available (open source) tools are limited
- Biggest advantage (personally):
  - IPv6 recap and new experiences gained in various domains
    - Ubuntu networking
    - Ostinato
    - Juniper SRX / Junos

Your Feedback

Any further questions?

AWK GROUP

Gabriel Müller
Dipl. El.-Ing. ETH
Senior Consultant

gabriel.mueller@awk.ch

Contents

MIBs

```
// mib-jnx-chassis.txt
// CPU Load RE
JUNIPER-MIB::jnxOperatingCPU.9.1.0.0
// RAM Load RE
JUNIPER-MIB::jnxOperatingBufferCP.9.1.0.0

// mib-jnx-js-spu-monitoring.txt
// CPU Load SPU
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsSPUMonitoringCPUUsage.0
// RAM Load SPU
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsSPUMonitoringMemoryUsage.0
// "Current IPv6 CP session number of SPU."
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsSPUMonitoringCPSessIPv6.0
// "Current IPv6 flow session number of SPU."
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsSPUMonitoringFlowSessIPv6.0
// "Node average IPv6 session created in last 96 seconds."
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsNodeSessCreationPerSecIPv6.0
```

For your Reference

MIBs

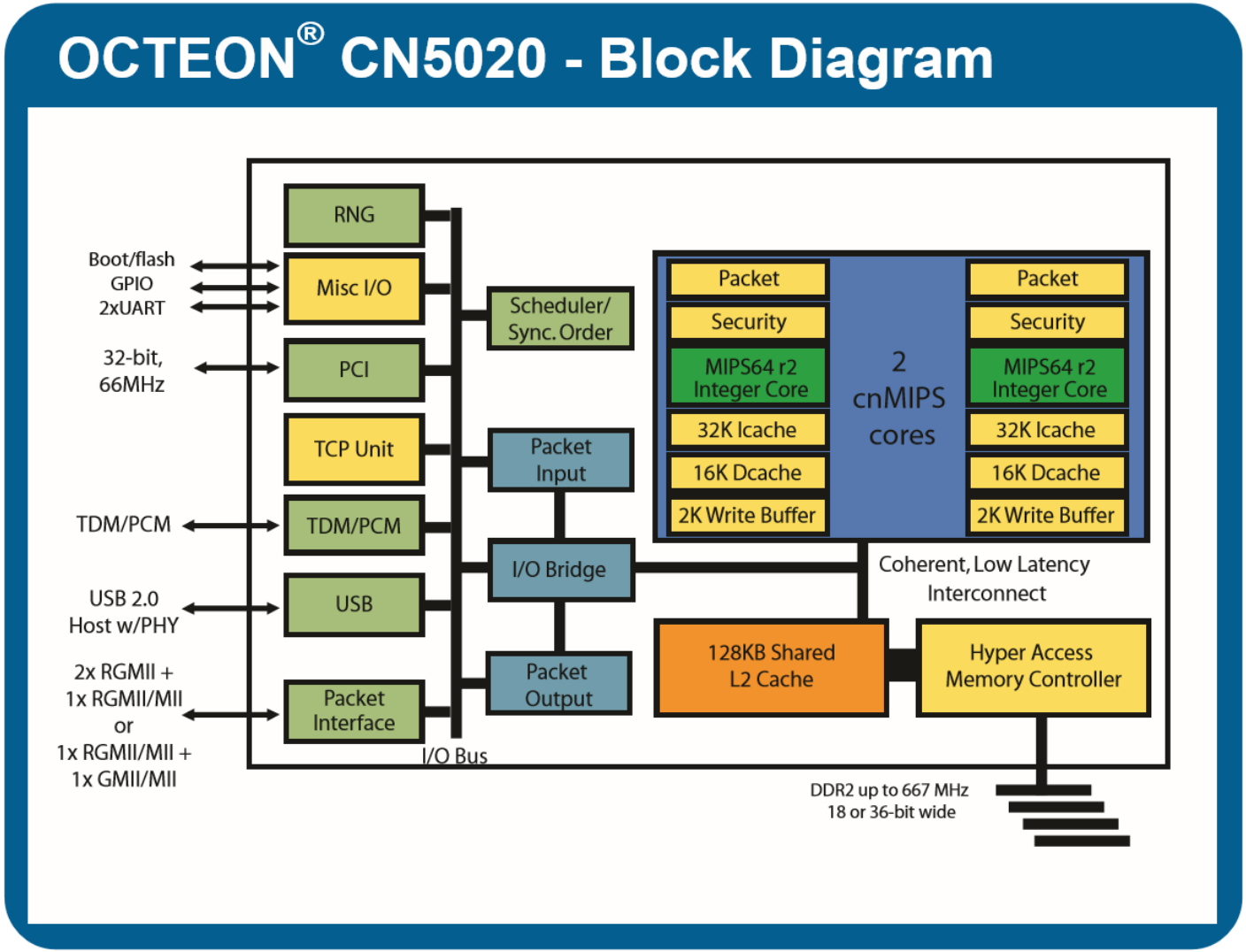
```
// "Node total IPv6 session in use."
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsNodeCurrentTotalSessIPv6.0
// "System level total IPv6 session in use."
JUNIPER-SRX5000-SPU-MONITORING-MIB::jnxJsSPUMonitoringTotalSessIPv6.0

// mib-jnx-jdhcpv6.txt
// DHCPv6
JUNIPER-JDHCPV6-MIB::jnxJdhcpv6LocalServerTotalDropped.0
JUNIPER-JDHCPV6-MIB::jnxJdhcpv6LocalServerSolicitReceived.0
JUNIPER-JDHCPV6-MIB::jnxJdhcpv6LocalServerRequestReceived.0
JUNIPER-JDHCPV6-MIB::jnxJdhcpv6LocalServerAdvertiseSent.0
JUNIPER-JDHCPV6-MIB::jnxJdhcpv6LocalServerReplySent.0

// mib-jnx-js-dns.txt
// DNS
JUNIPER-JS-DNS-MIB::jnxJsDNSProxyQueriesReceived.0
JUNIPER-JS-DNS-MIB::jnxJsDnsProxyResponsesSent.0
JUNIPER-JS-DNS-MIB::jnxJsDnsProxyQueriesForwarded.0
JUNIPER-JS-DNS-MIB::jnxJsDnsProxyNegativeResponses.0
JUNIPER-JS-DNS-MIB::jnxJsDnsProxyRetryRequests.0
JUNIPER-JS-DNS-MIB::jnxJsDnsProxyPendingRequests.0
JUNIPER-JS-DNS-MIB::jnxJsDnsProxyServerFailures.0
```

For your Reference

Data Collection - Script

```
#!/bin/bash
# $1 -> File name
# $2 -> Sleeping time
while :
do
date +%s%3N | tr '\n' ',' >> $1
snmpget -v 2c -c public -O Uqv 10.1.10.101 <OID-1> <OID-2> … | tr '\n' ',' >> $1
echo >> $1
sleep $2
done
```

SRX-210HE2 – CPU Architecture



Source: https://cavium.com

For your Reference

Other Open Source Tools

- Data Plane Development Kit (DPDK)
  - *"Data Plane Development Kit (DPDK) greatly boosts packet processing performance and throughput, allowing more time for data plane applications. DPDK can improve packet processing performance by up to ten times. DPDK software running on current generation Intel® Xeon® Processor E5-2658 v4, achieves 233 Gbps (347 Mpps) of L3 forwarding at 64-byte packet sizes."*
    - http://www.intel.com/content/www/us/en/communications/data-plane-development-kit.html

- TRex – Realistic traffic generator
  - *"TRex is an open source, low cost, stateful traffic generator fuelled by DPDK. It generates L4-7 traffic based on pre-processing and smart replay of real traffic templates. TRex amplifies both client and server side traffic and can scale to 200Gb/sec with one UCS. New TRex now supports Stateless functionality, multiple streams, ability to change any packet field and provides per stream statistics, latency and jitter."*
    - https://trex-tgn.cisco.com/

- Various Tools
    - http://resources.infosecinstitute.com/15-best-free-packet-crafting-tools/