Traffic Analysis Report

by

Sonny Brar

Customer

Contents

Customer

Introduction

Customer is one of Canada's leading business law firms, recognized for top tier services in each of our core practice areas - corporate finance, M&A, real estate, corporate-commercial law, banking, structured finance, tax, insolvency, competition and foreign investment, employment and business litigation. They are regularly retained by domestic and international companies in a wide range of industries including financial services, insurance, technology, telecommunication, transportation, manufacturing, mining, energy, infrastructure and retail.

The firm's Canadian offices are leaders in their respective jurisdictions. [redacted] The firm is also well known for its extensive regulatory and government relations expertise; the latter anchored by its office in Ottawa.

Customer engaged my company to perform a detailed traffic analysis of their network traffic that would provide them with an understanding of the amount of bandwidth used by protocols and applications running on their network. Professional Services (PS) monitored the relevant WAN circuit with Wireshark and the captured files were used to analyse and provide a snapshot of the network during those times.

Summary of Findings

A Professional Services (PS) consultant performed a detailed analysis of the captured data and concluded the following:

1. The Average bandwidth used on the Link is 19.50Mb/s
2. The Peak rate for small data bursts is a bit over 60Mb/s
3. The Average packet size is around 545 bytes
4. MS Networking protocols (all protocols used by MS) take about 48% of the total used bandwidth
5. Voice and Video use about 9% of the total used bandwidth
6. Web traffic takes about 23% of the total used bandwidth
7. Email consumes around 5.8% followed by Database with 1.60% of the total used bandwidth
8. Unknown traffic types consume around 12% of the total used bandwidth
9. TCP and IP are the main transport and network protocols used
10. The busiest subnet is 172.16.9.0 followed by 172.16.8.0
11. 172.16.9.120 is the Top IP Talker
12. Top TCP source port used is 445(Microsoft-DS)
13. Top TCP source port used is 514 (syslog) followed by 51798

Bandwidth Over Time

Source File: E:\Pilot\121218.pcap

File Size: 433088KB

Bytes per Second

The number of bytes per second on the monitored link

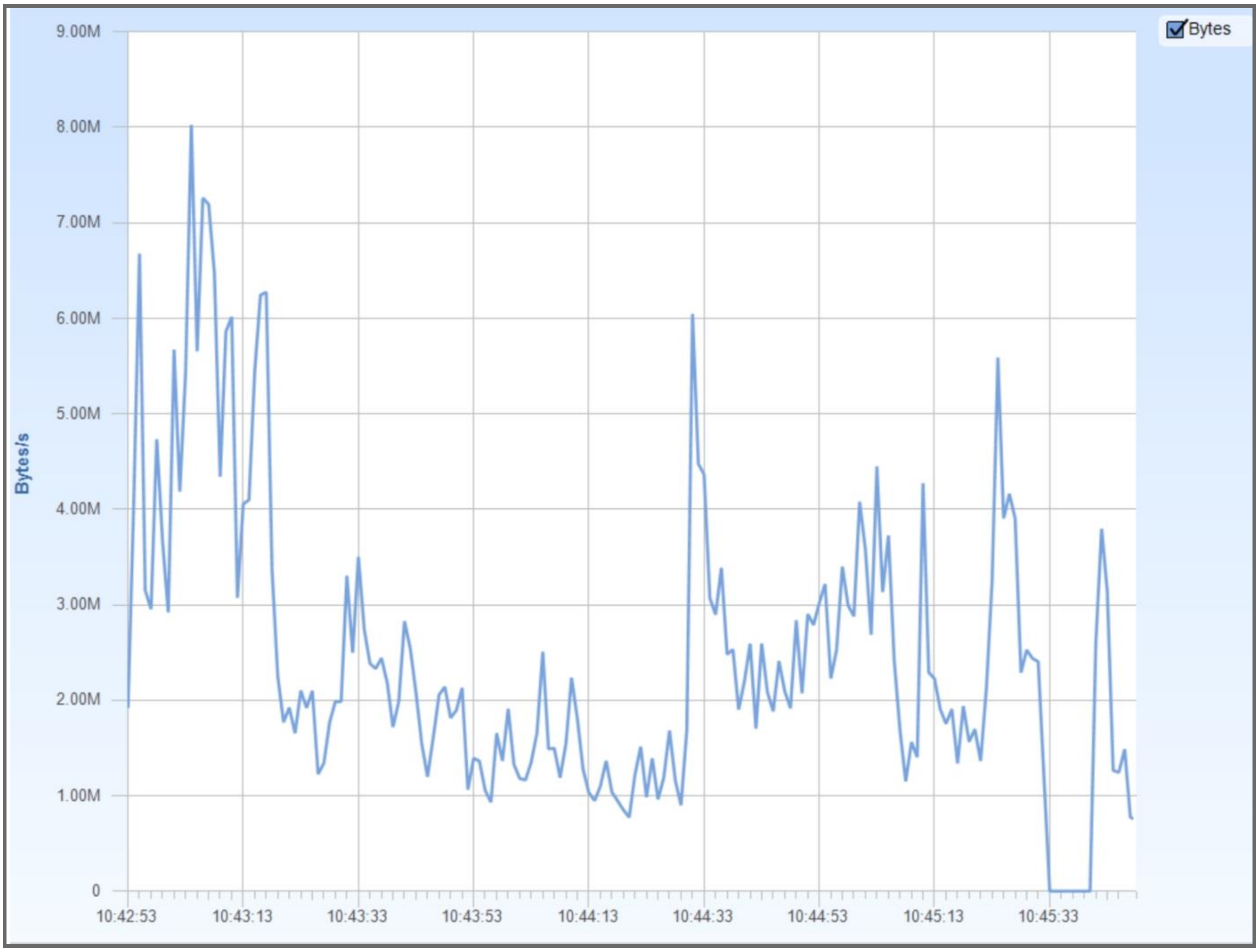


Figure 1 - Bytes per Second

Bits per Second

The number of bits per second. This enables an at-a-glance view of the total bandwidth used as well as a detailed look in single second precision.

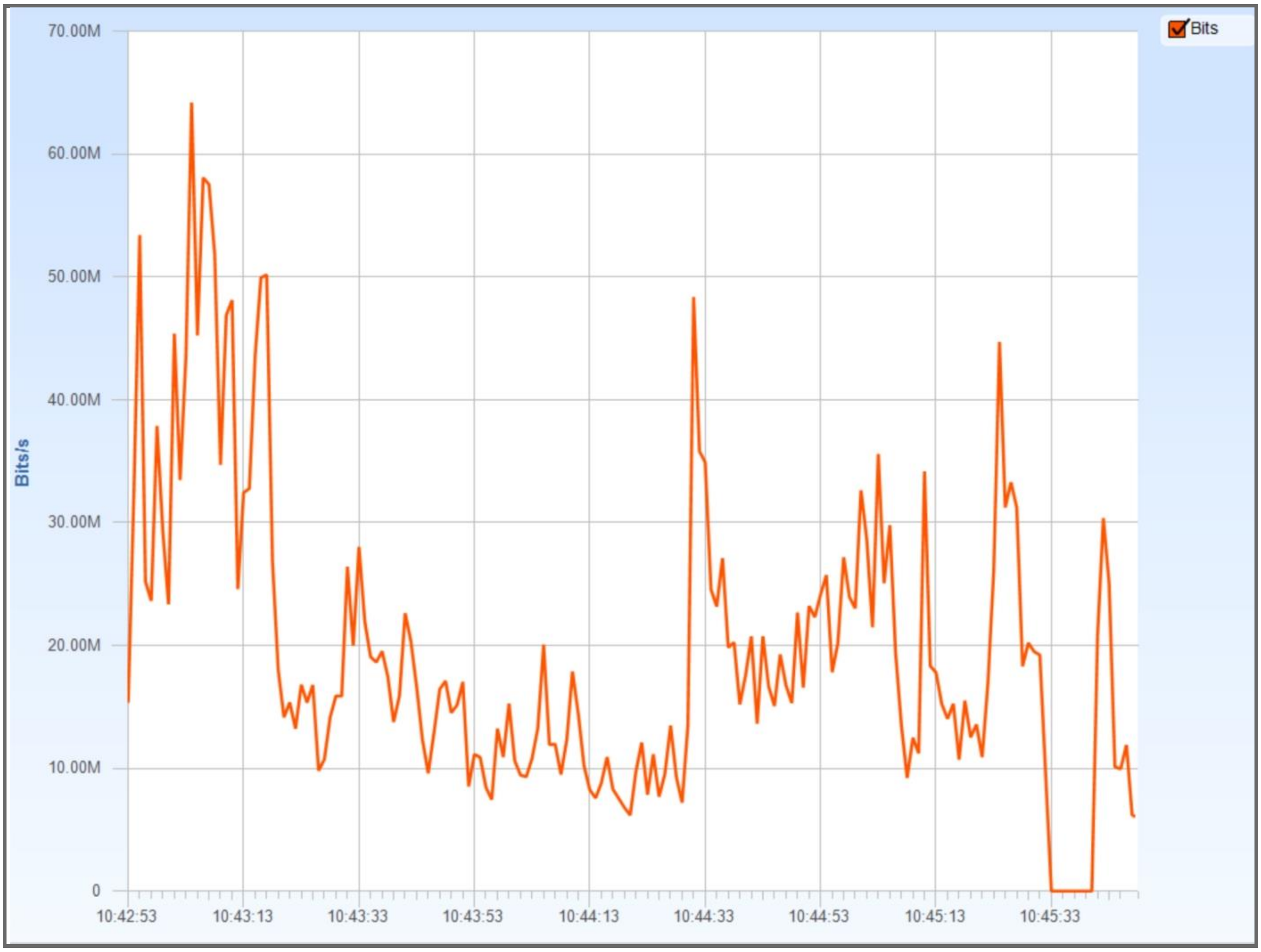


Figure 2 - Bits per Second

Packets per Second

The number of packets per second. This view when compared to the bits/bytes view above allows the user to visually identify when many small packets are generating the traffic or if it is a few larger packets.

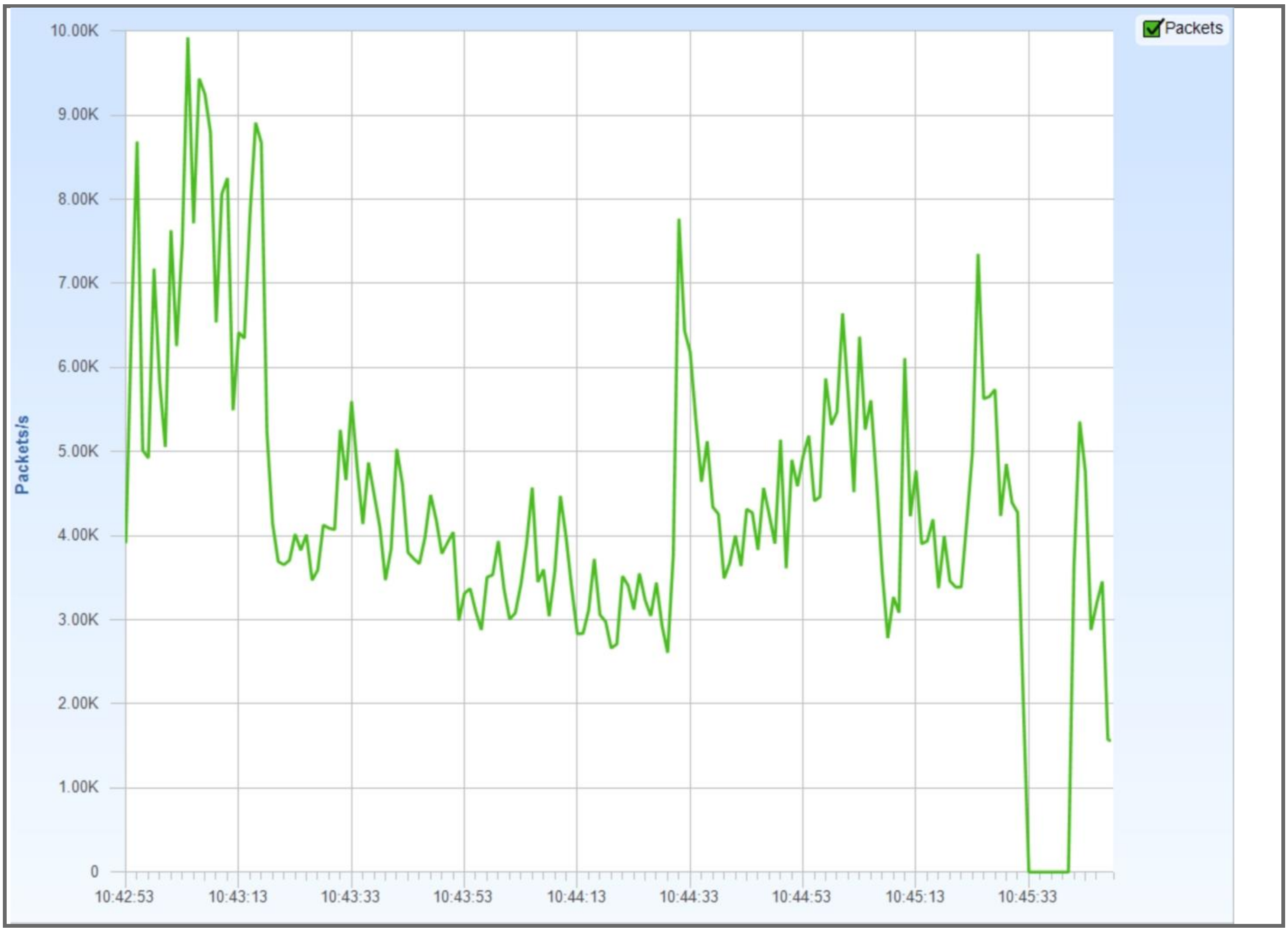


Figure 3 - Packets per Second

Bits Over Time

Amount of bits per second for each type of network traffic, charted over time.

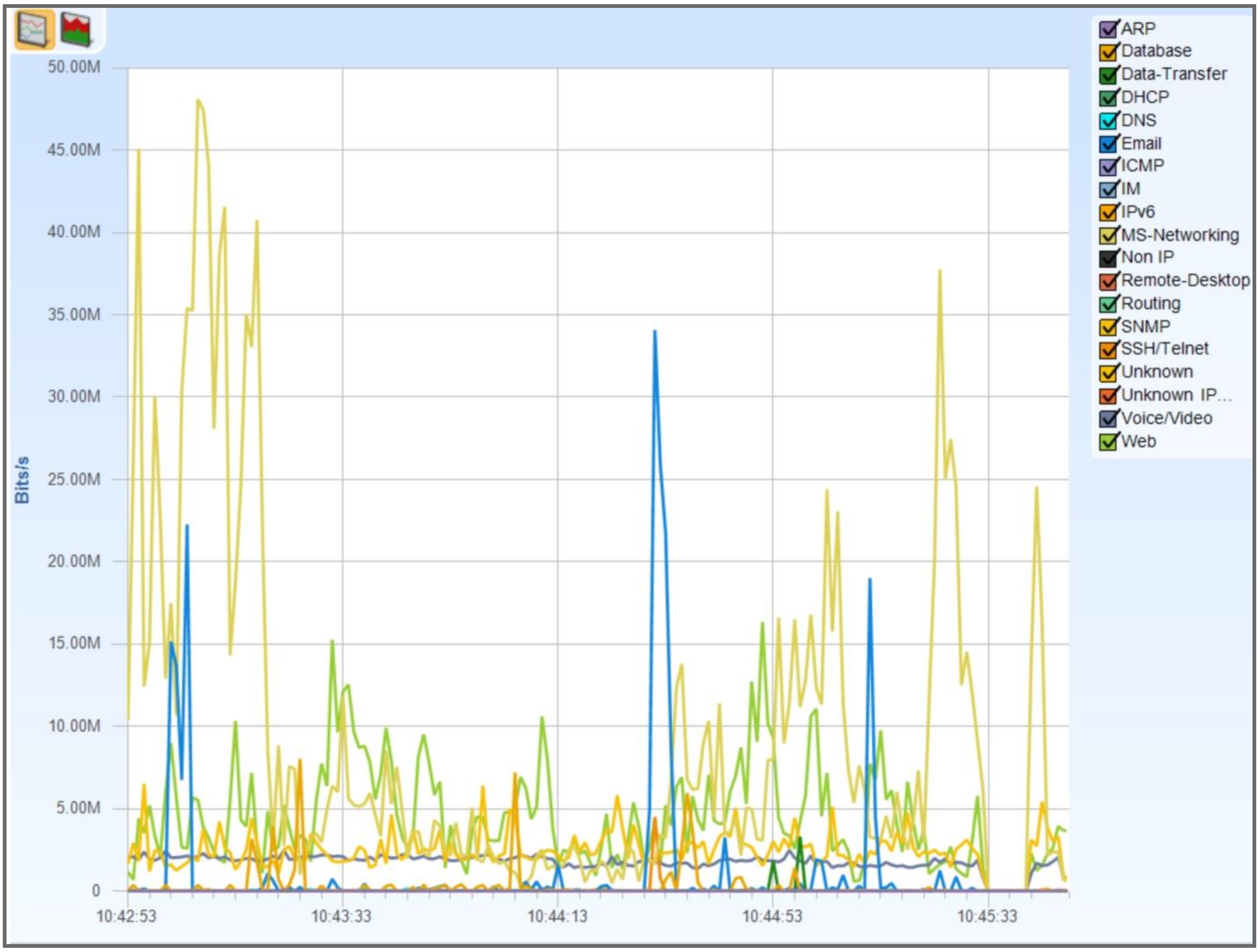


Figure 4 - Bits Over Time

Total Bits

Total network usage for the different types of network traffic, during the visualized time interval.

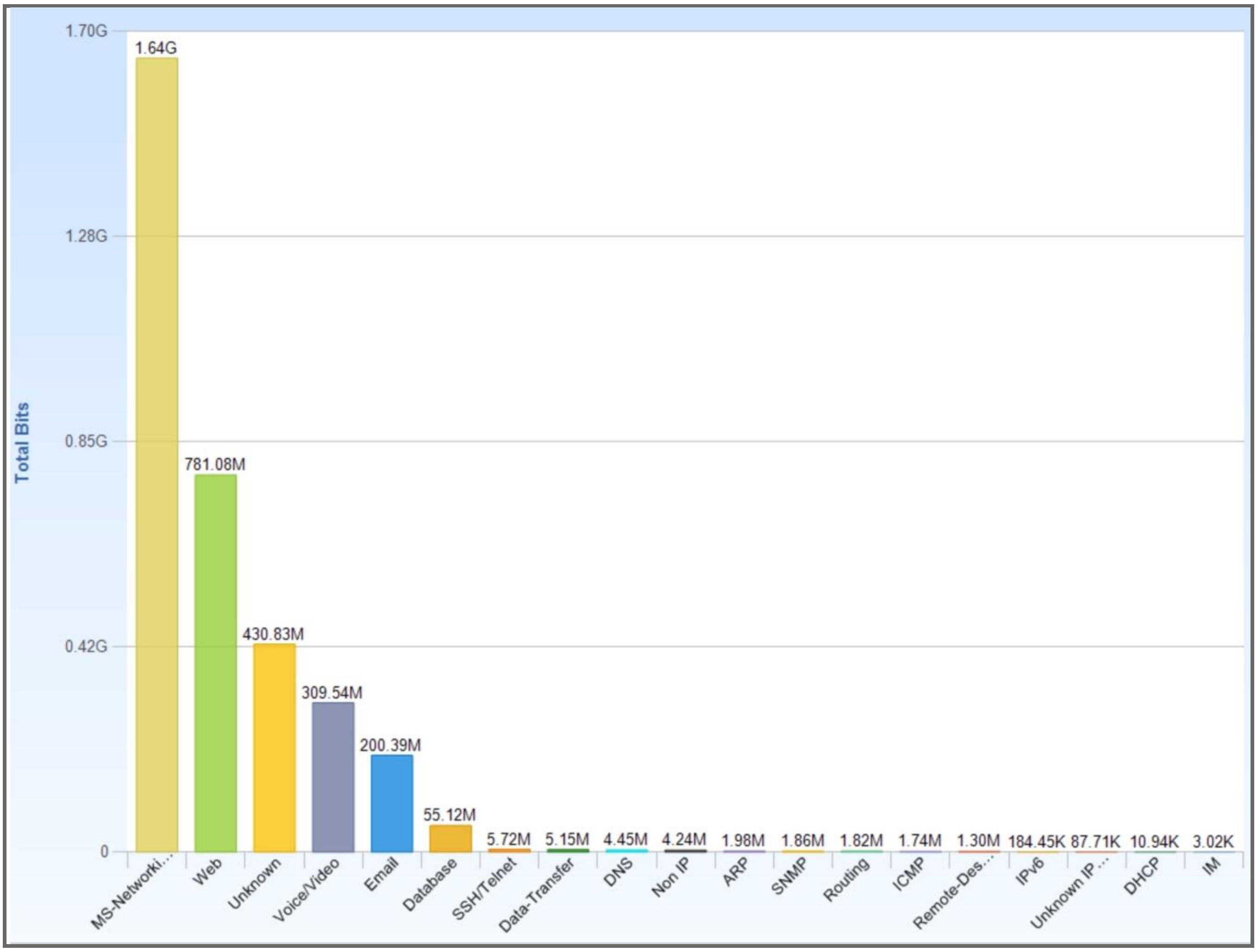
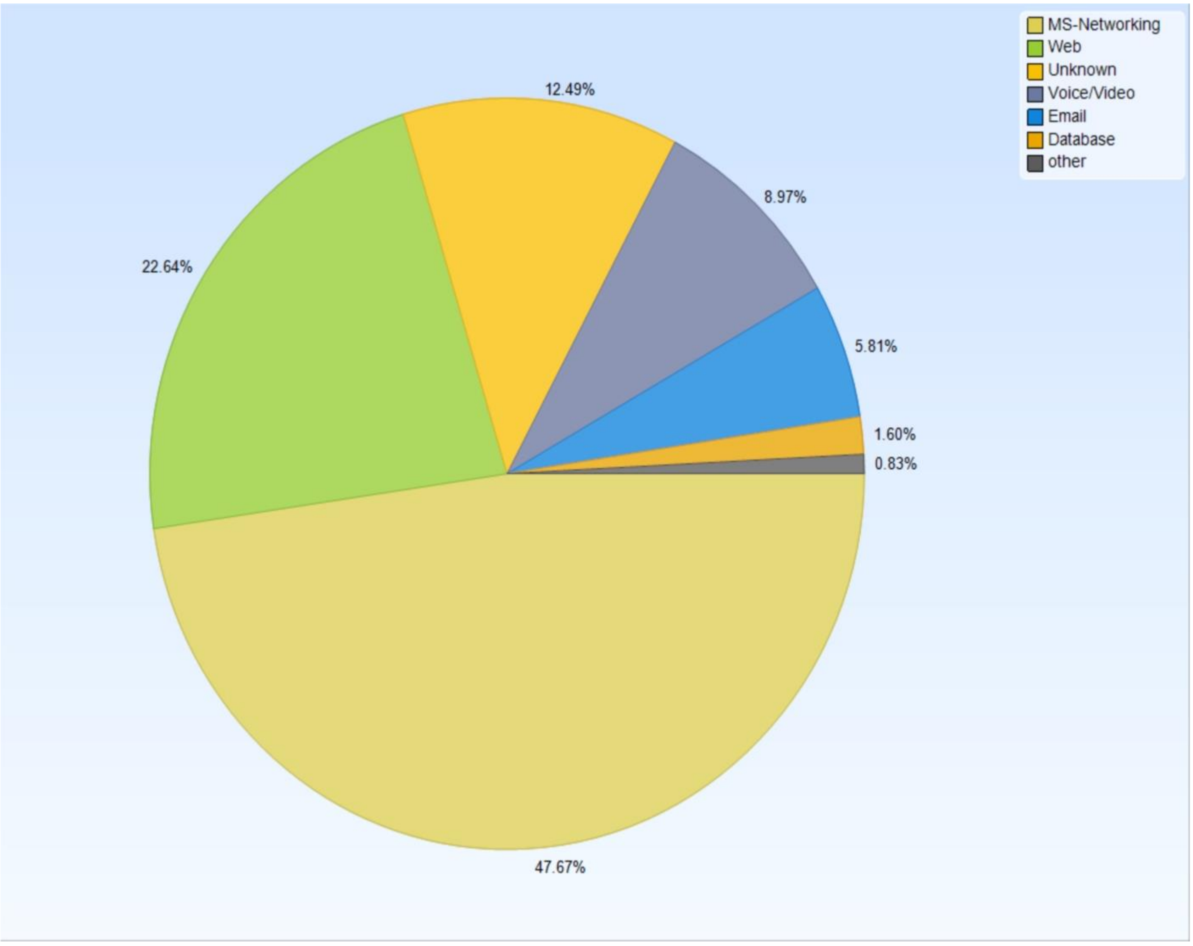


Figure 5 - Total Bits

Relative Network Usage

Relative network usage for the different types of network traffic, during the visualized time interval.



IP Conversations

Conversations among IP hosts

IP Conversations

IP host conversations. The size of the host is relative to the amount of data it has transmitted. The size of each connection is relative to how much traffic it has transported between the two endpoints (hosts).

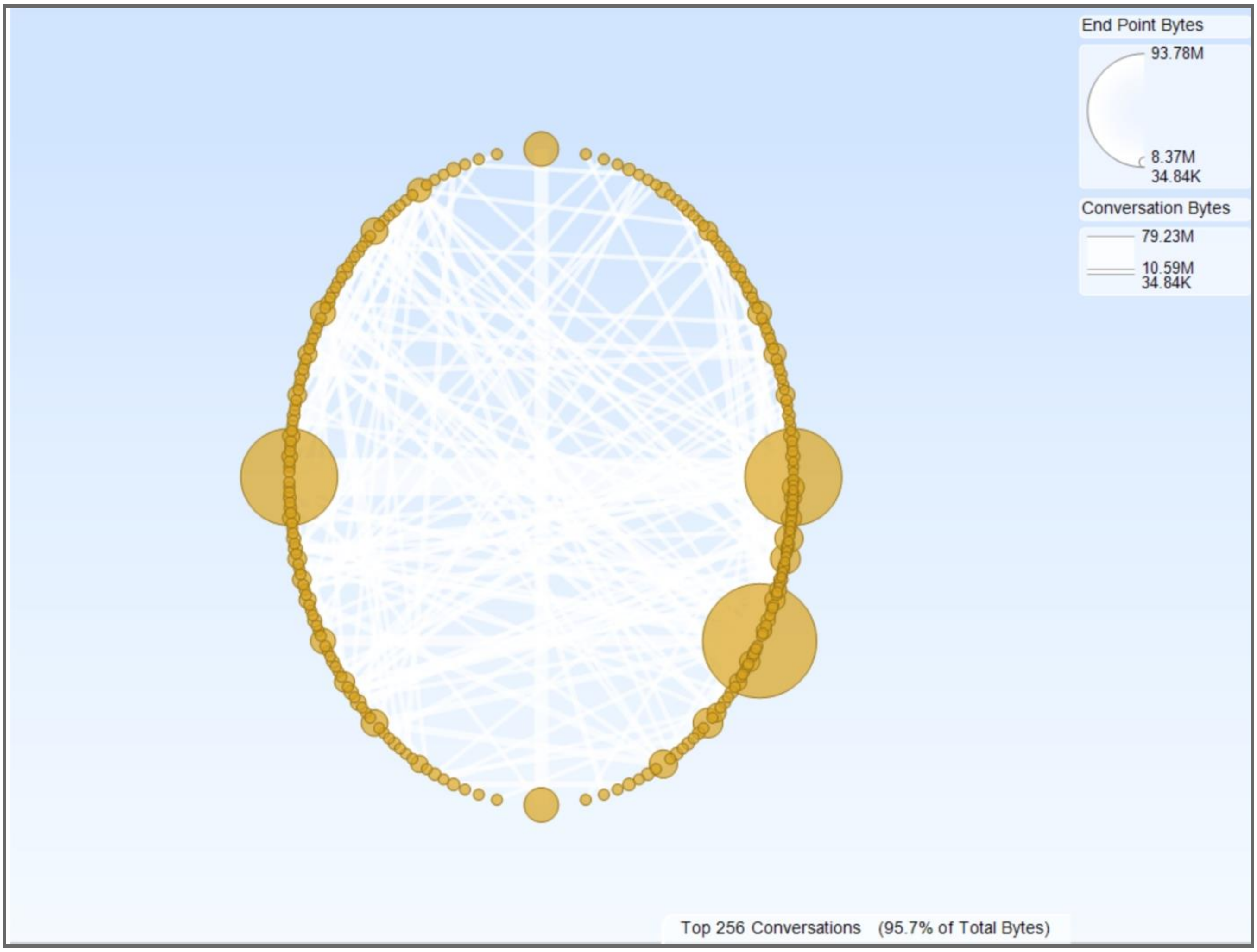


Figure 7 - IP Conversations

Protocol Distribution - Bits

Overview of protocol subdivisions at different layers, based on total Bits

Network Protocols

Total bits aggregated by network layer protocol, e.g. IP, IPv6, ARP.

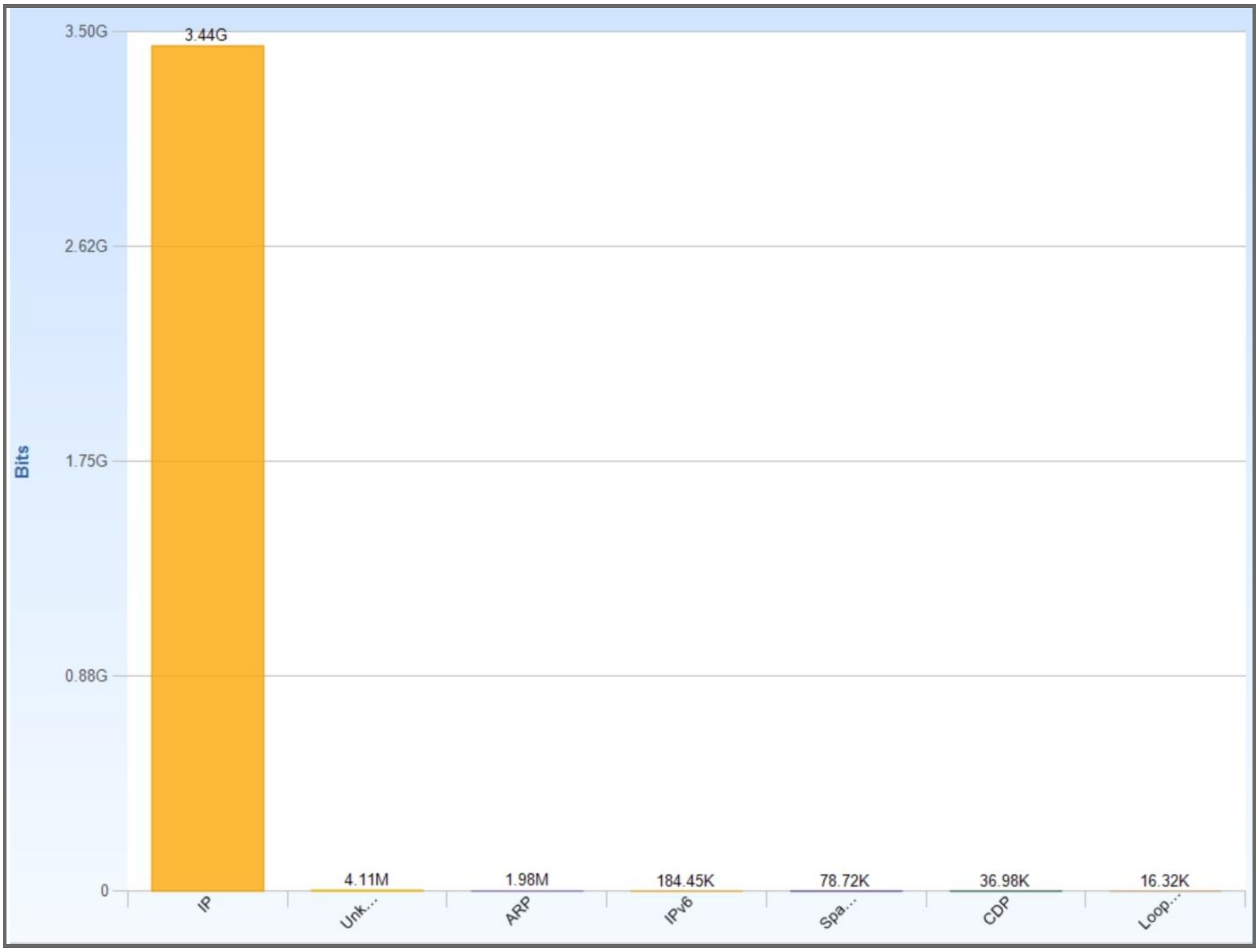


Figure 8 - Network Protocols

Transport Protocols

Total bits aggregated by transport layer protocol, e.g. TCP, UDP, ICMP.

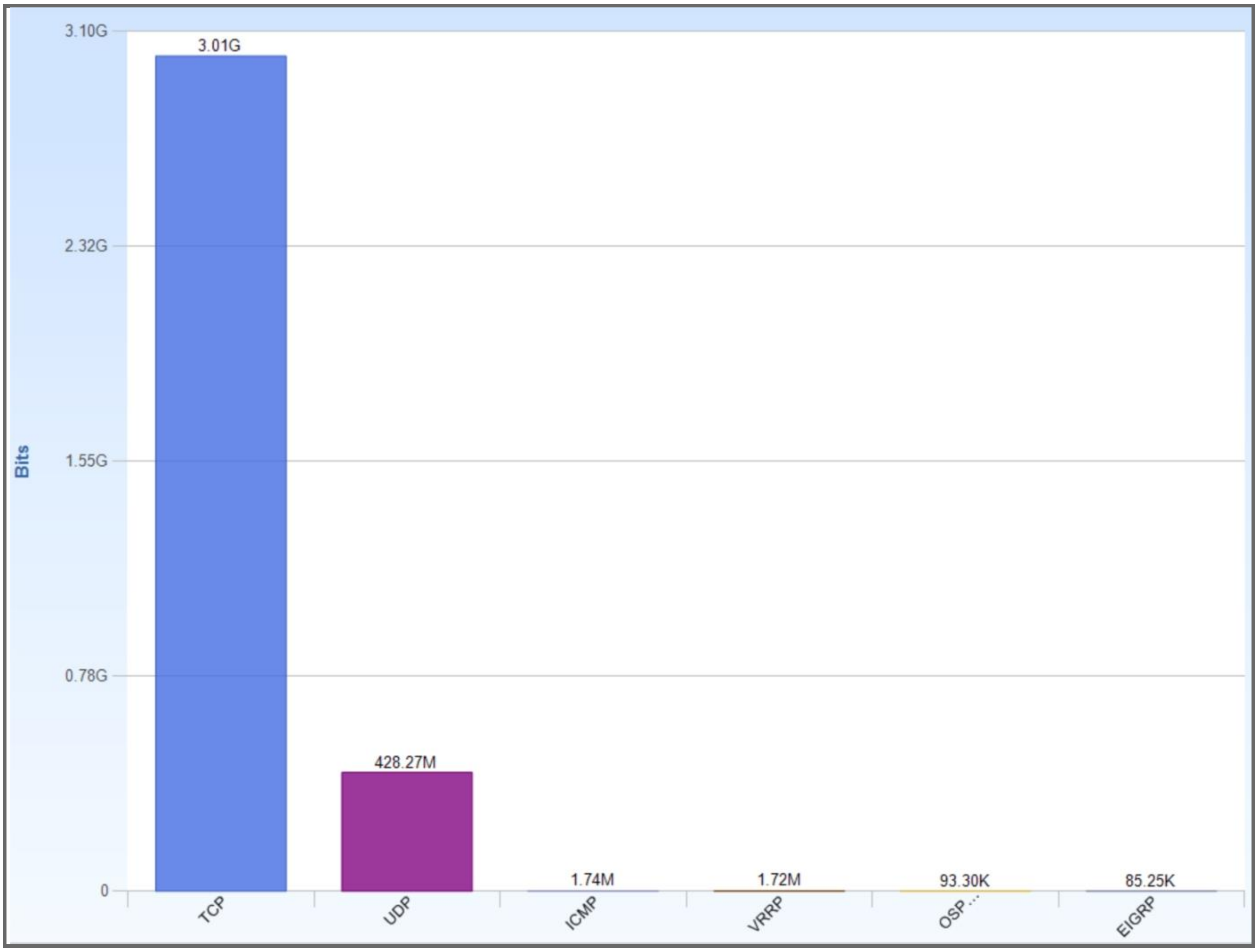


Figure 9 - Transport Protocols

TCP Protocols

Total bits aggregated by TCP port, e.g. HTTP, POP3.

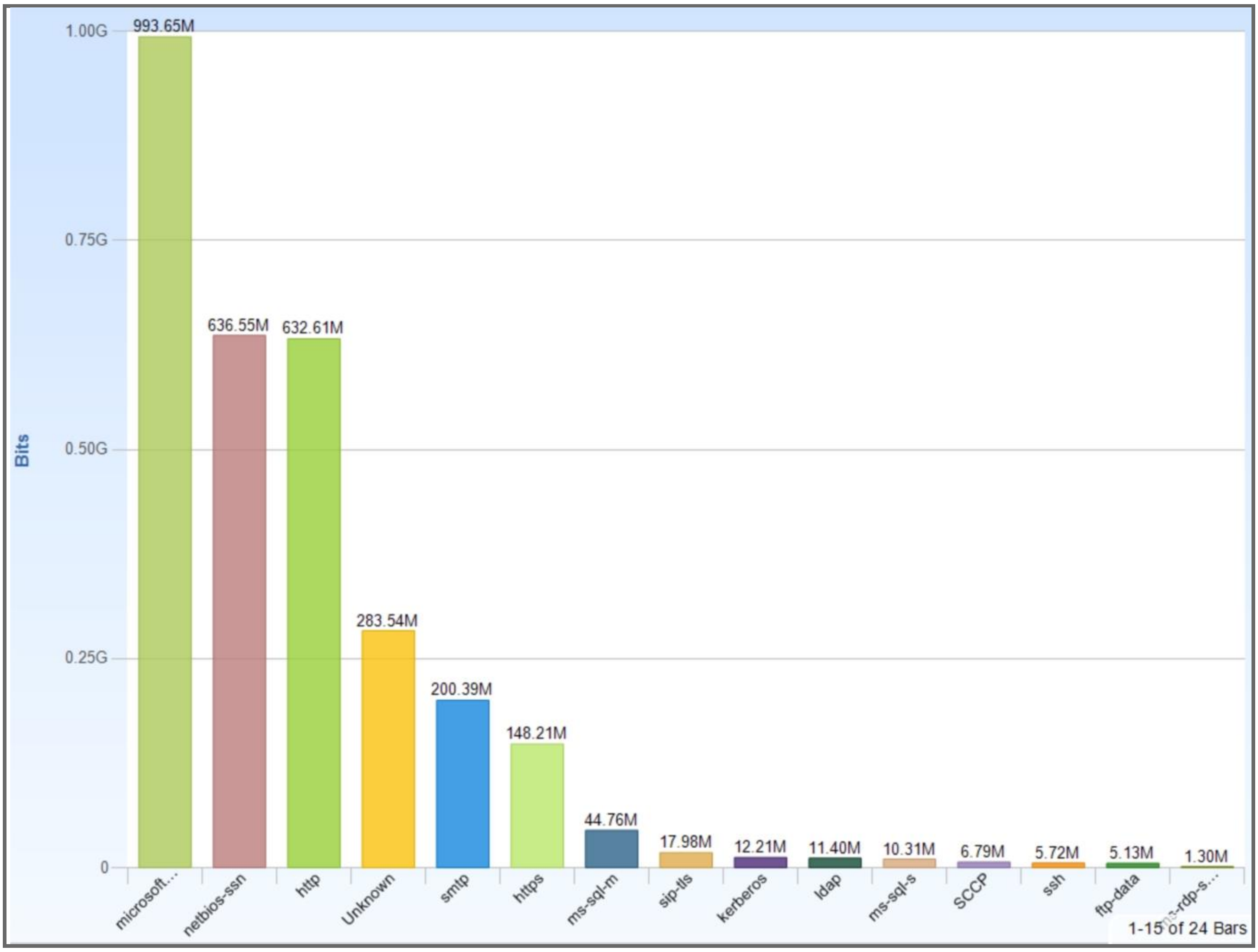


Figure 10 - TCP Protocols

UDP Protocols

Total bits aggregated by UDP port, e.g. DNS, DHCP.

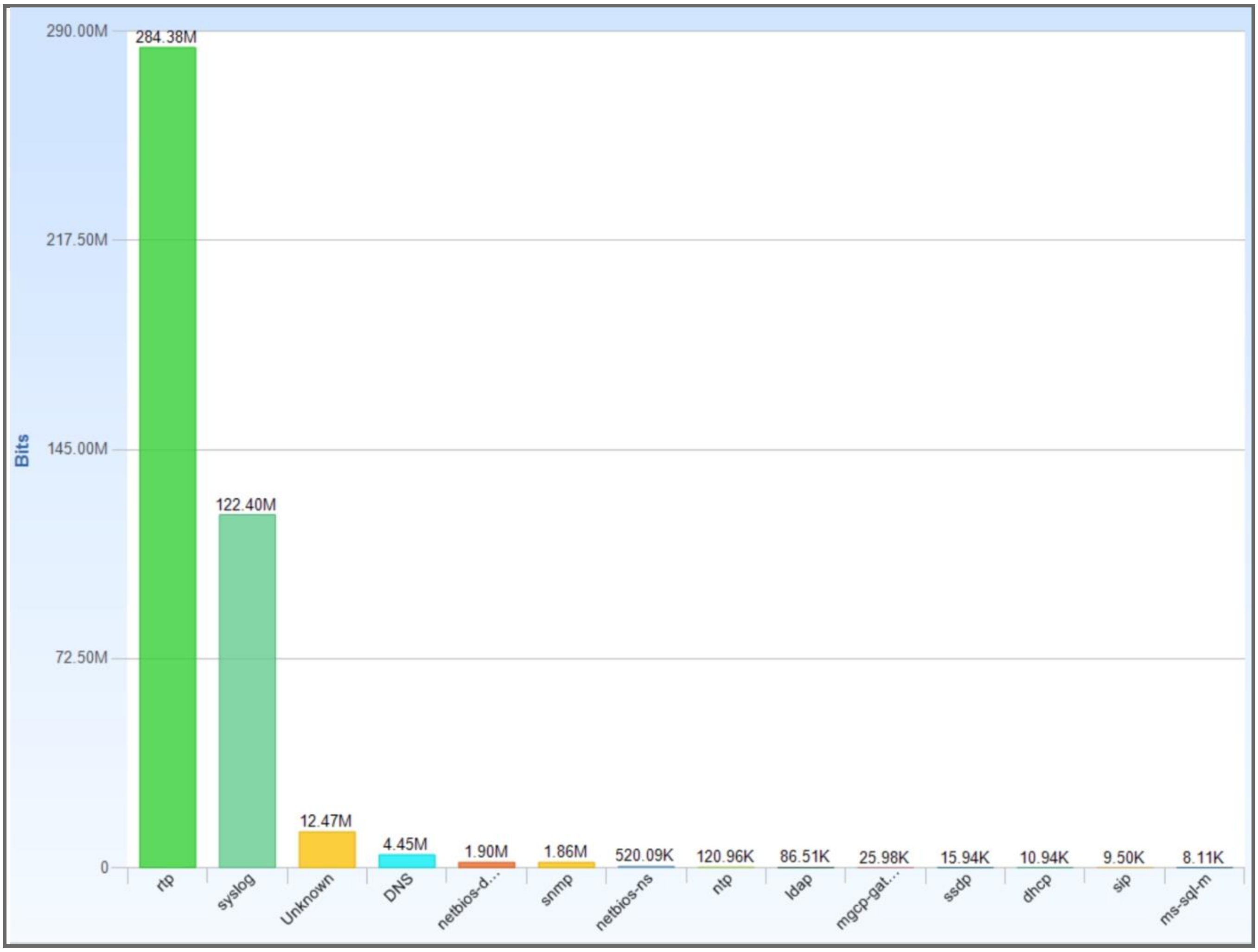


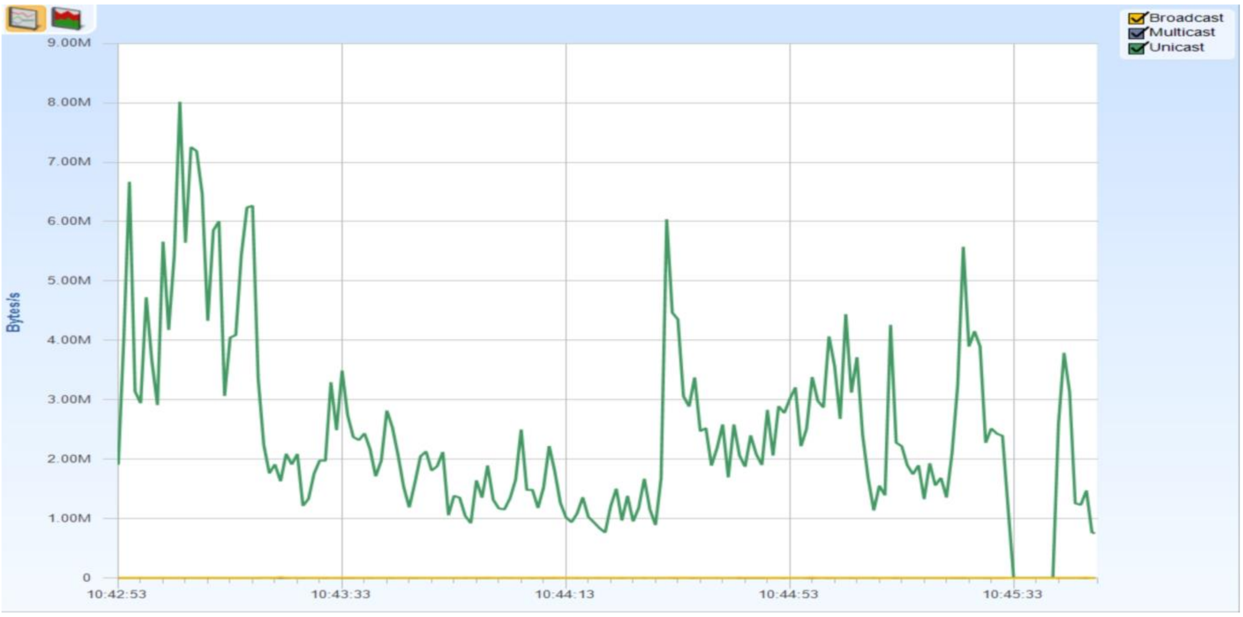
Figure 11 - UDP Protocols

Unicast vs. Multicast vs. Broadcast Traffic

Unicast vs. Multicast vs. Broadcast Traffic Analysis

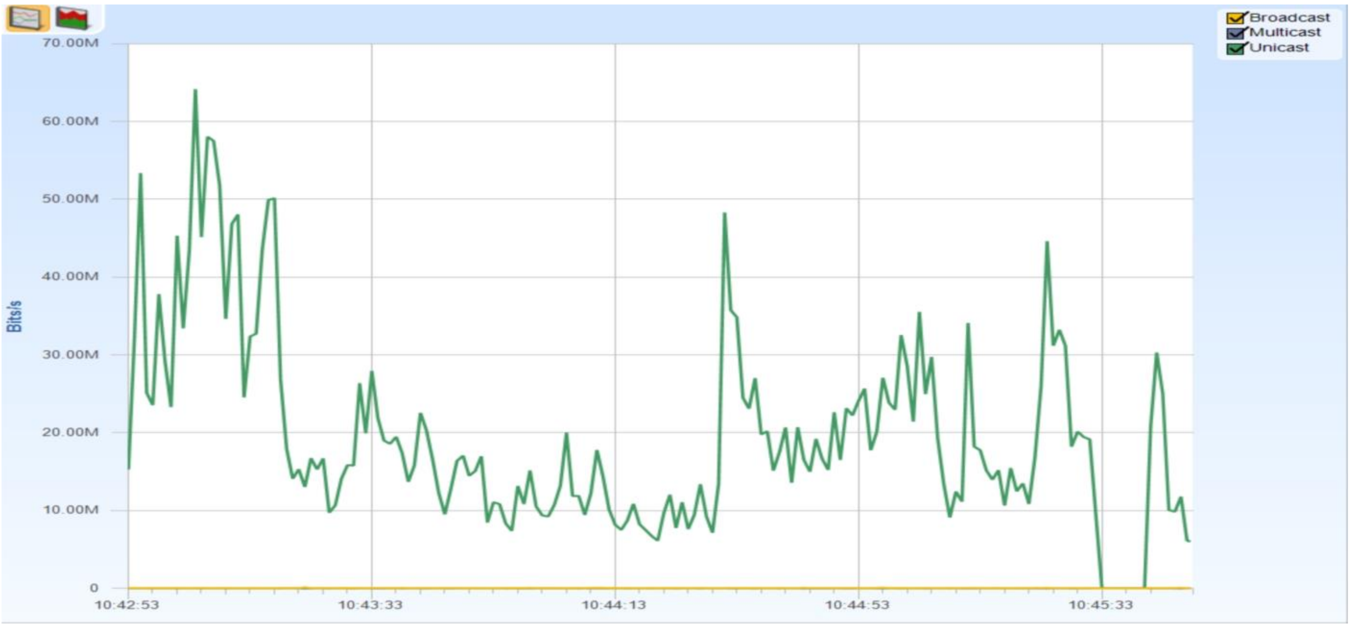
Bytes per Second

Unicast, multicast and broadcast bandwidth usage, in bytes per second.



Bits per Second

Unicast, multicast and broadcast bandwidth usage, in bits per second.



Packets per Second

Unicast, multicast and broadcast bandwidth usage, in packets per second.

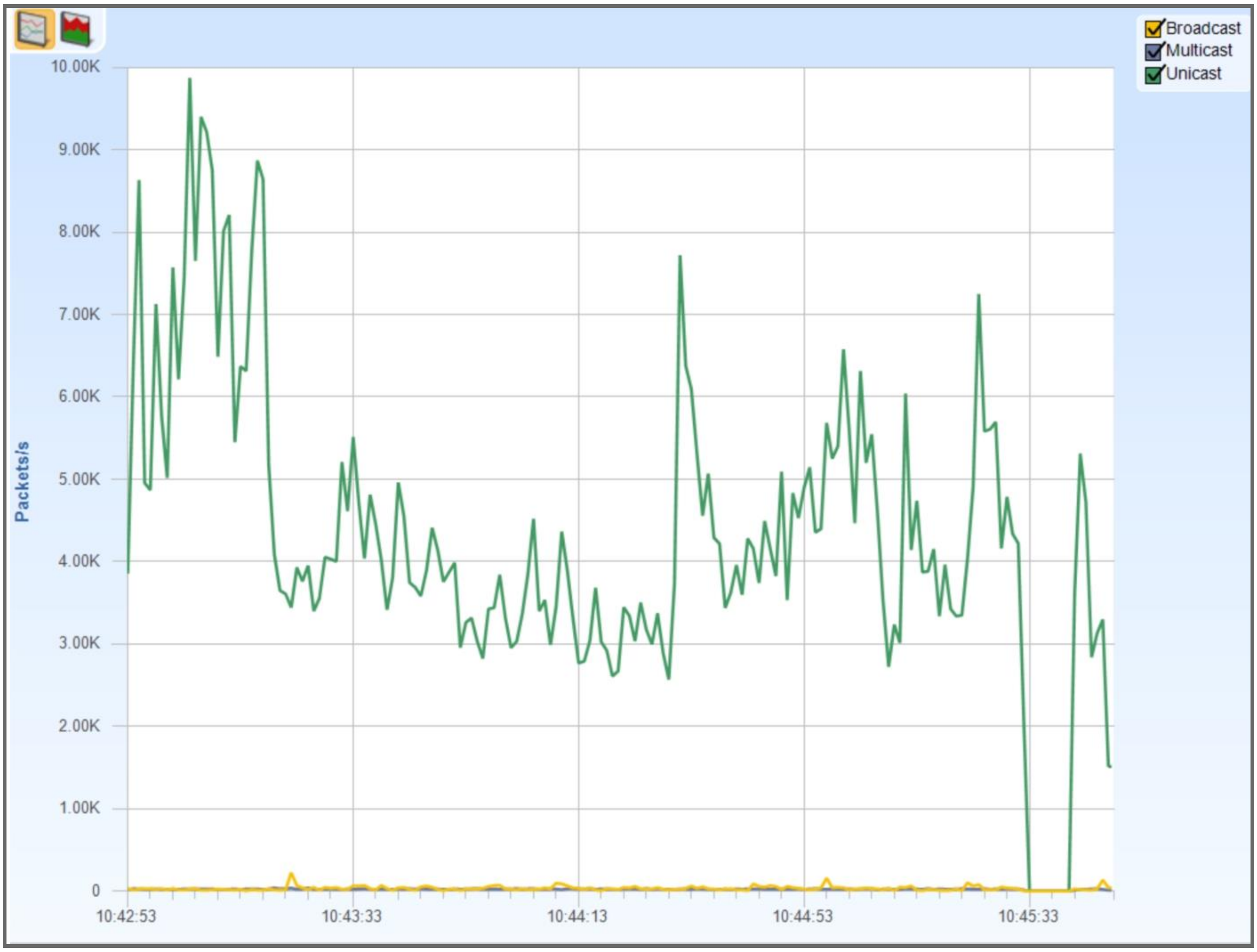


Figure 14 - Packets per Second

Total Unicast vs Multicast vs Broadcast Traffic

Relative percentage of unicast, multicast and broadcast traffic.

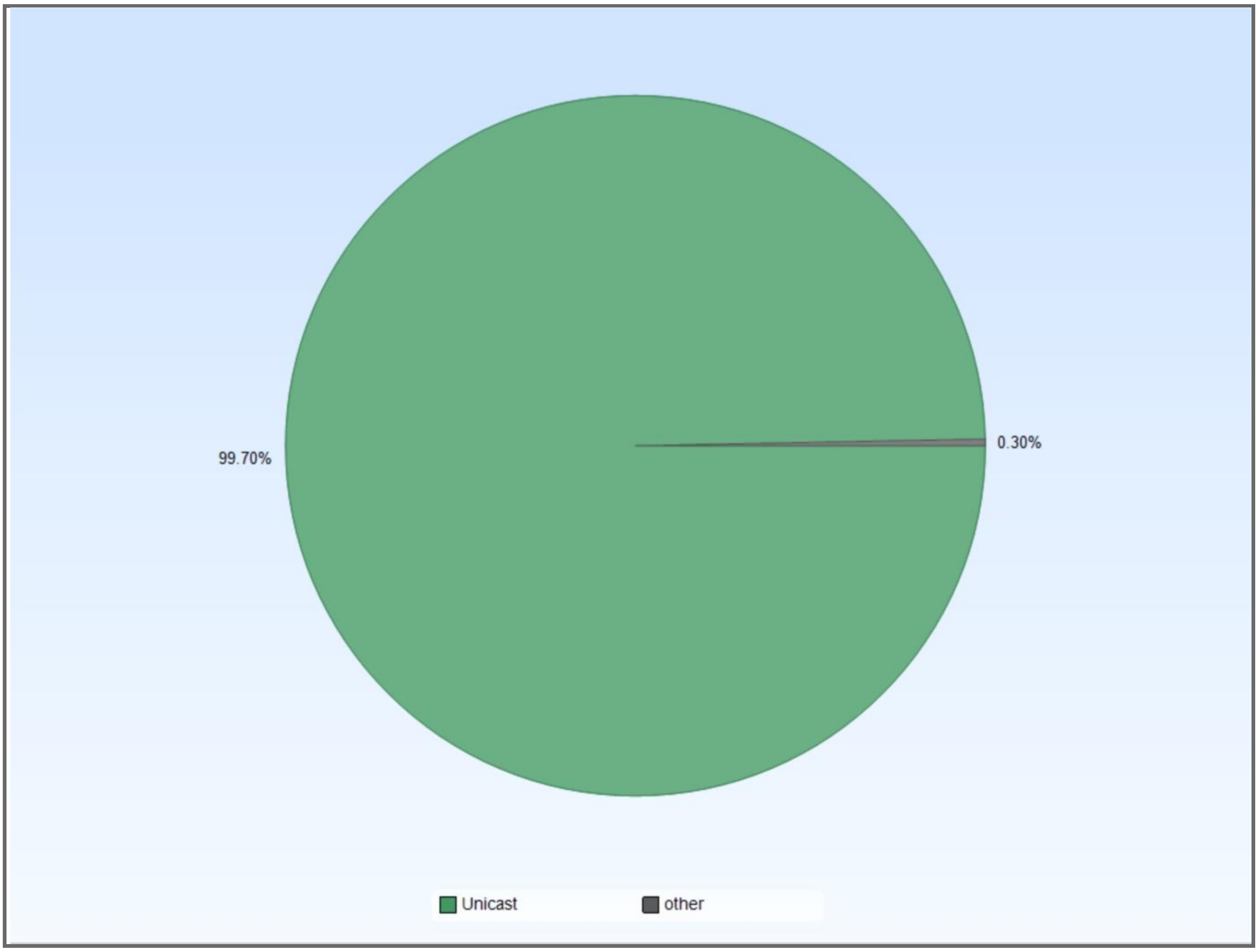


Figure 15 - Total Unicast vs Multicast vs Broadcast Traffic

Network Usage Summary by Direction and Traffic Type

Network usage summary, categorized by traffic type, for the different directions (i.e. local network to external network).

All Traffic

Amount of bits transfered on the network for the different traffic types.

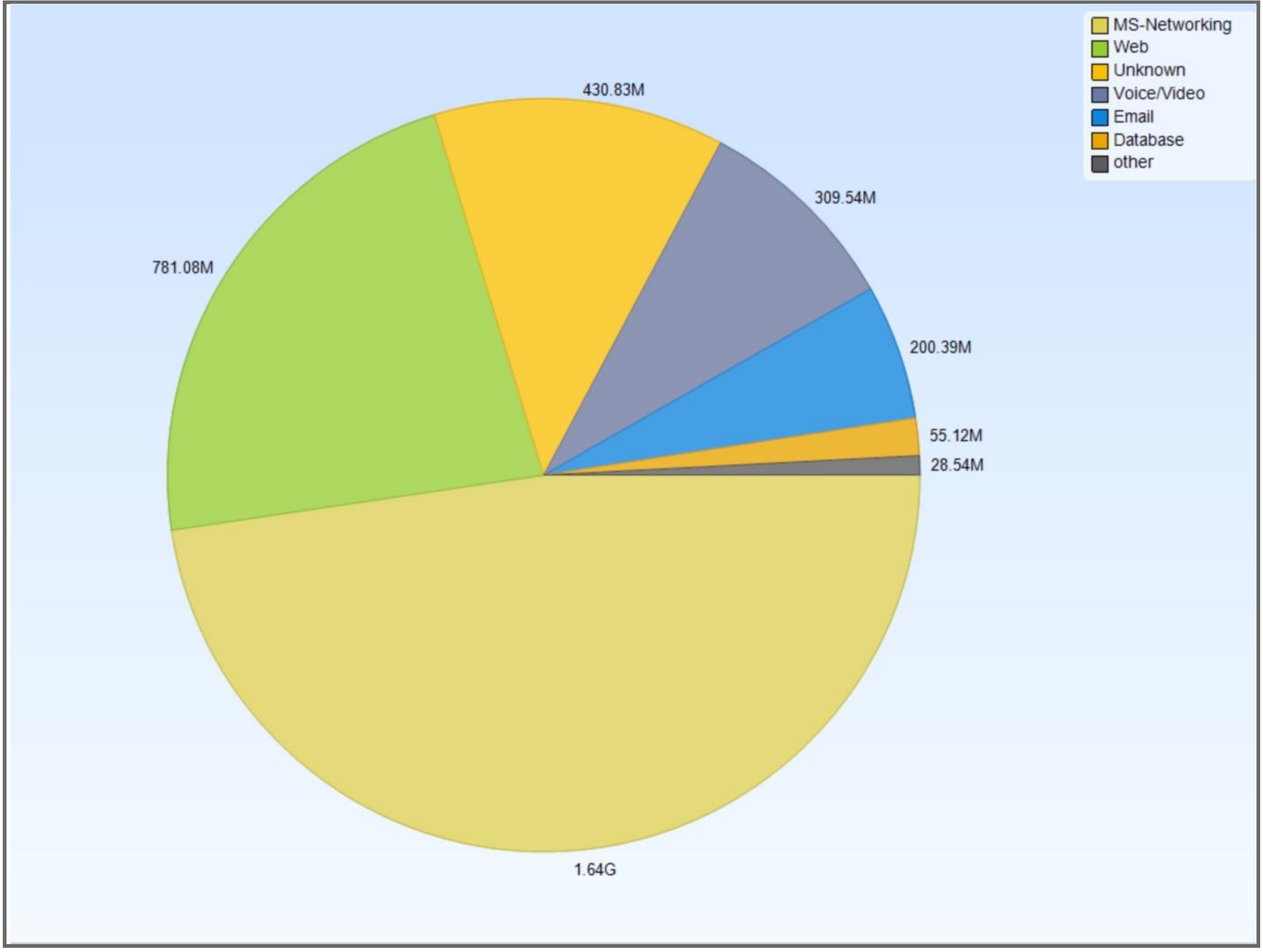


Figure 16 - All Traffic

Incoming Traffic (External Sender to Local Receiver)

Amount of bits that go from the external world to the local network, for the different traffic types.

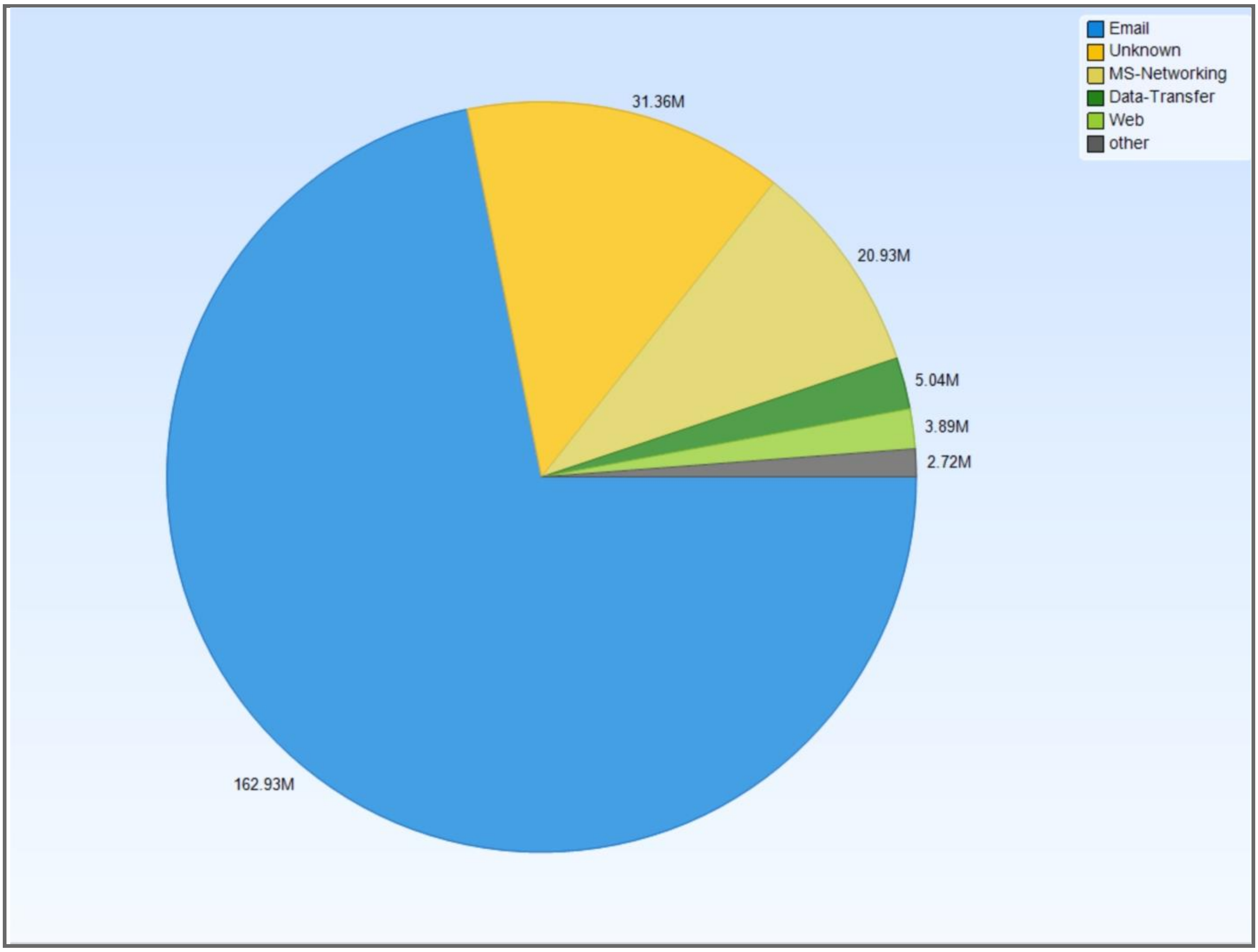


Figure 17 - Incoming Traffic (External Sender to Local Receiver)

Outgoing Traffic (Local Sender to External Receiver)

Amount of bits that go from the local network to the external world, for the different traffic types.

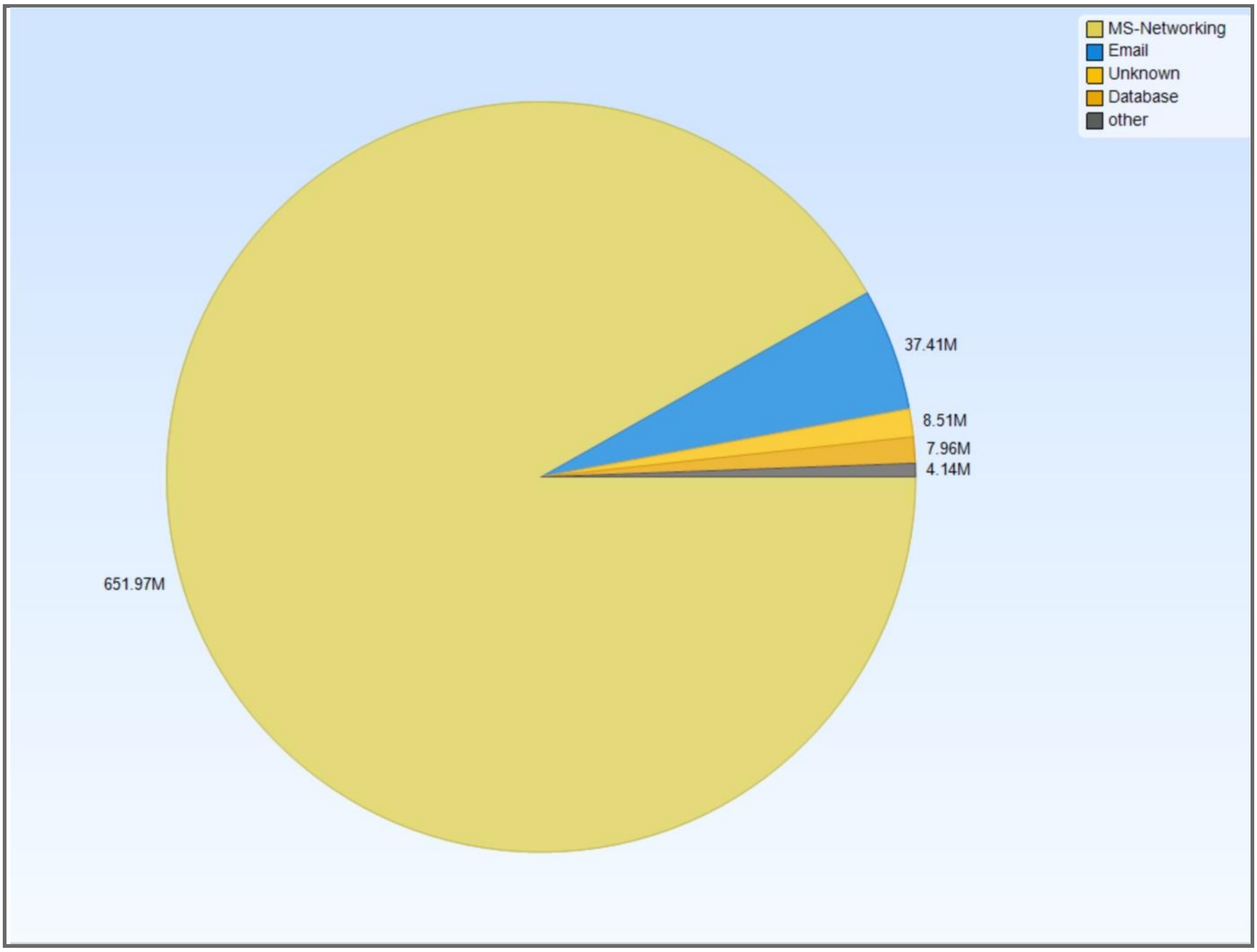


Figure 18 - Outgoing Traffic (Local Sender to External Receiver)

Top IP Talkers

Top IP Talkers. Each entry includes the traffic sent and received by the host.

Top Talkers - Packets

Top IP Talkers in packets.

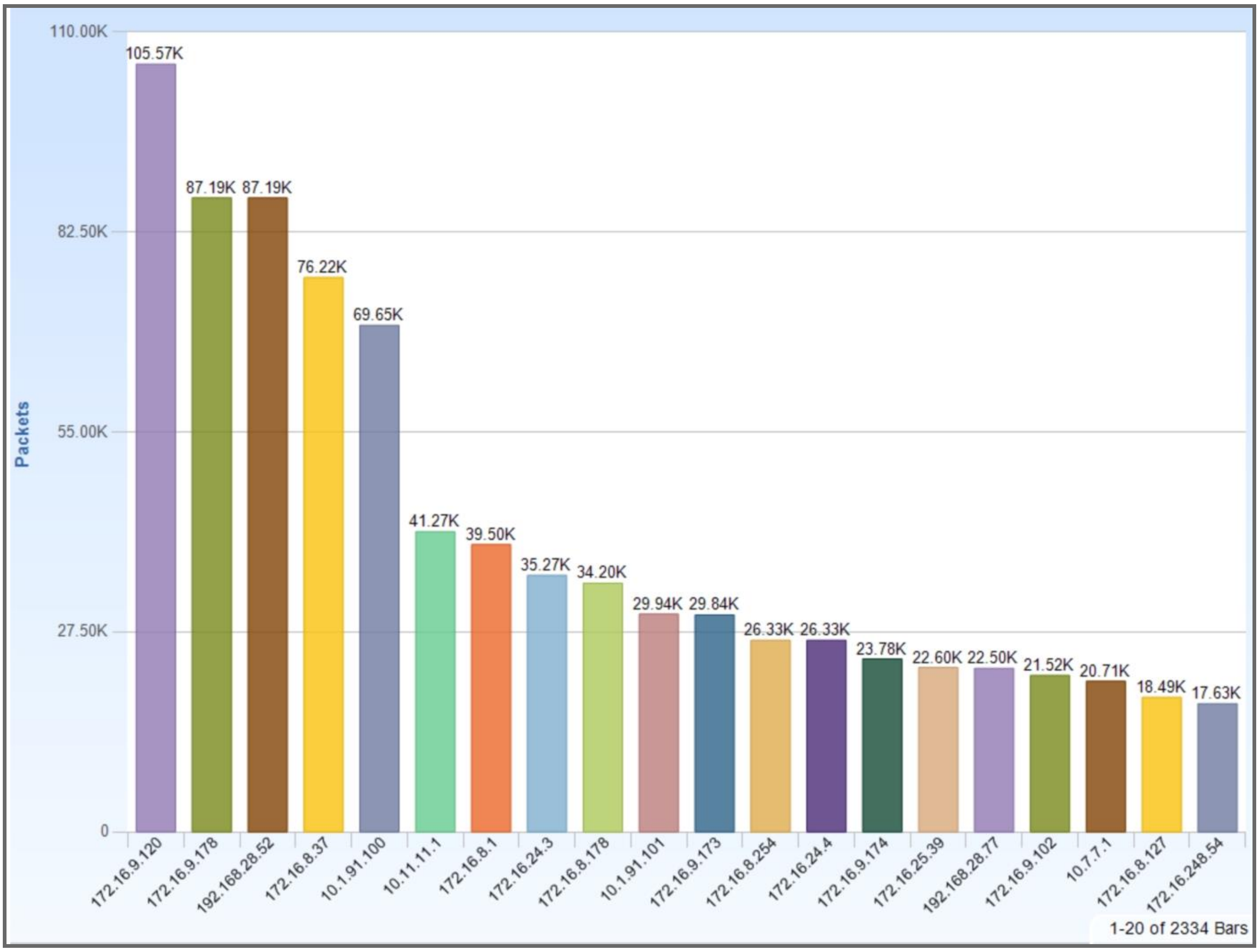


Figure 19 - Top Talkers - Packets

Top Talkers - Bytes

Top IP Talkers in bytes.

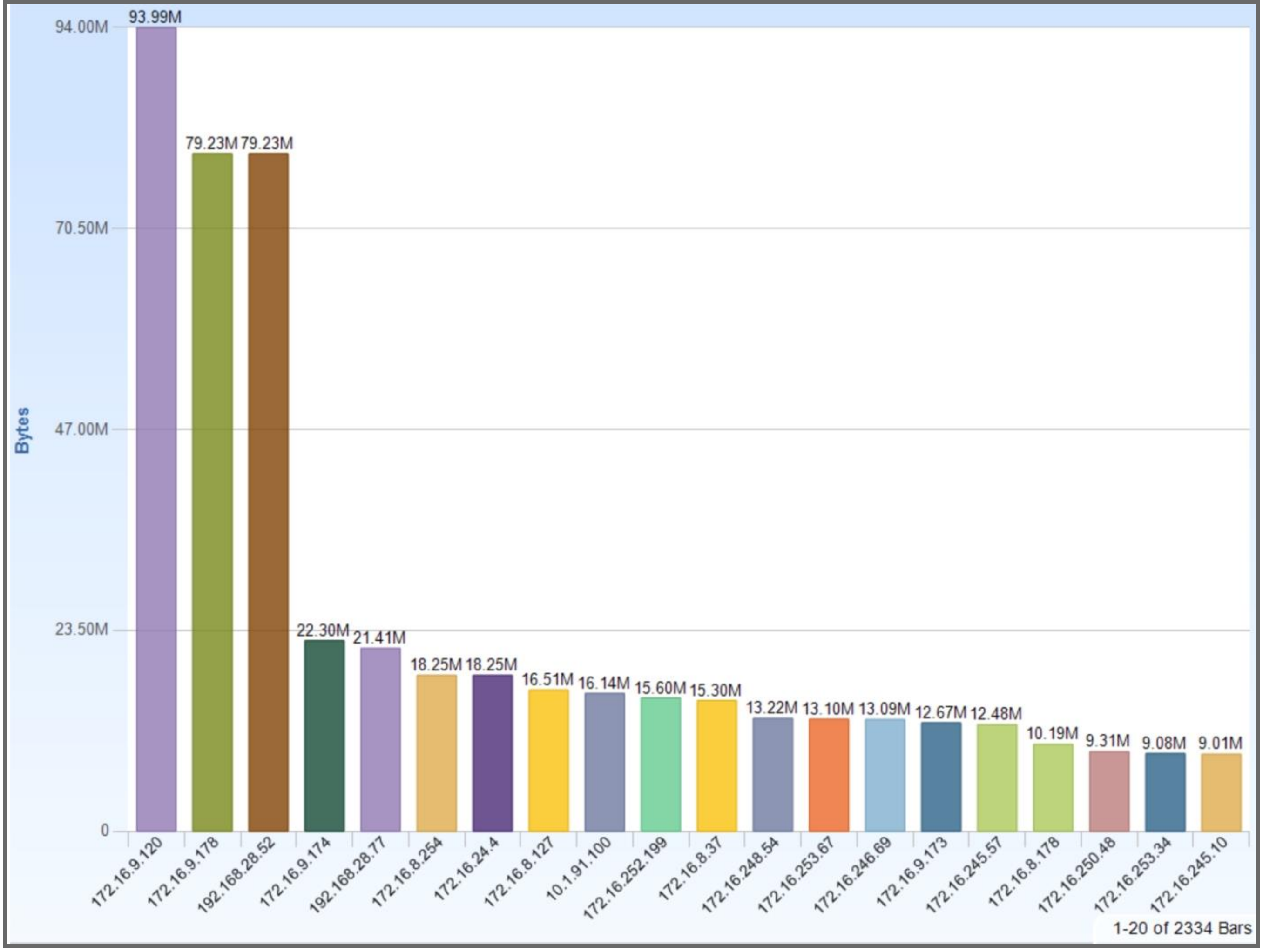


Figure 20 - Top Talkers - Bytes

Top Talkers - Bits

Top IP Talkers in bits.

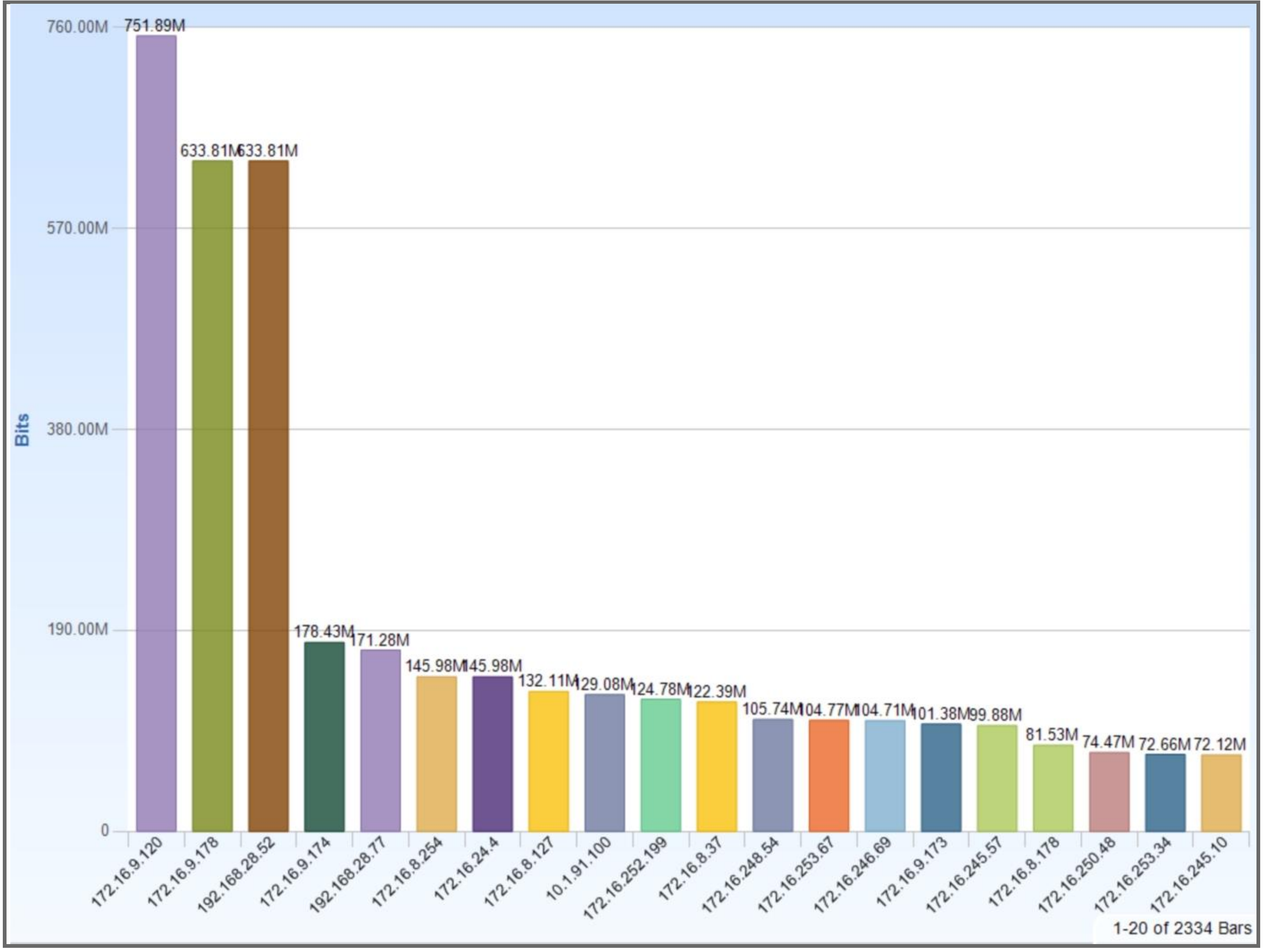


Figure 21 - Top Talkers - Bits

Top Source Ports

Top TCP-UDP source ports, based on the amount of bits, bytes or packets

TCP Bytes

Top TCP source ports, ordered by total sent bytes.

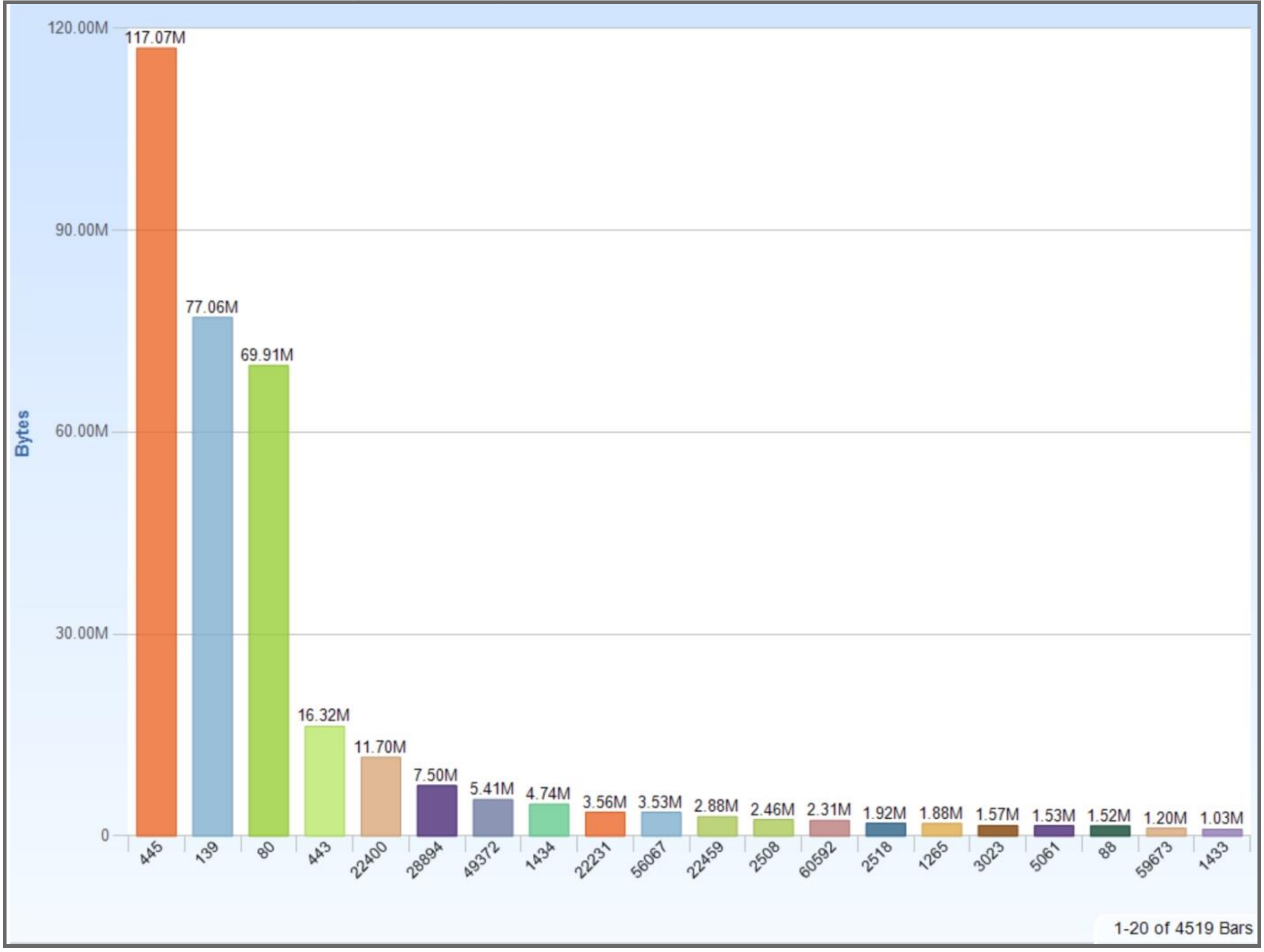
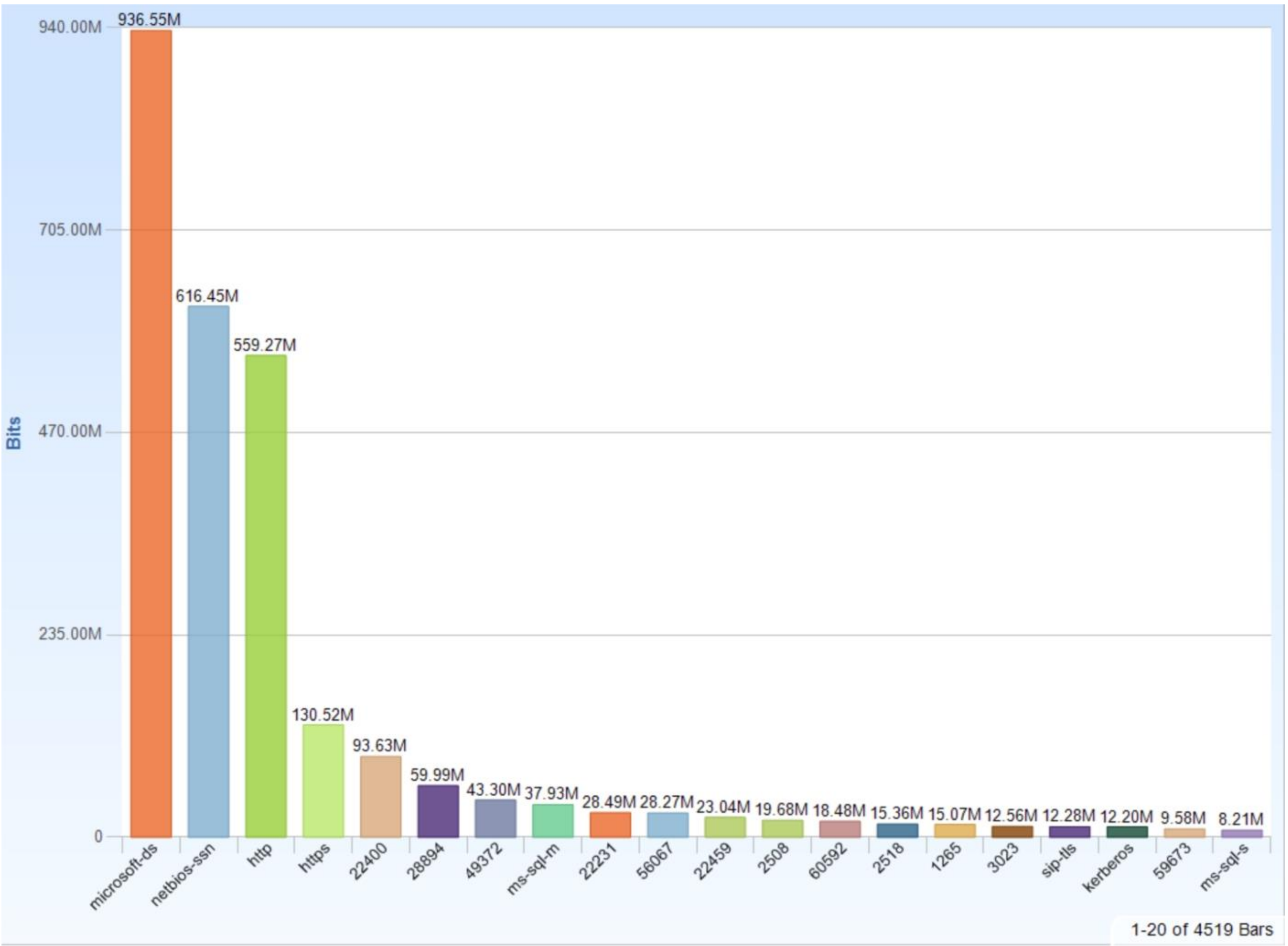


Figure 22 - TCP Bytes

TCP Bits

Top TCP source ports, ordered by total sent bits.



TCP Packets

Top TCP source ports, ordered by total sent packets.

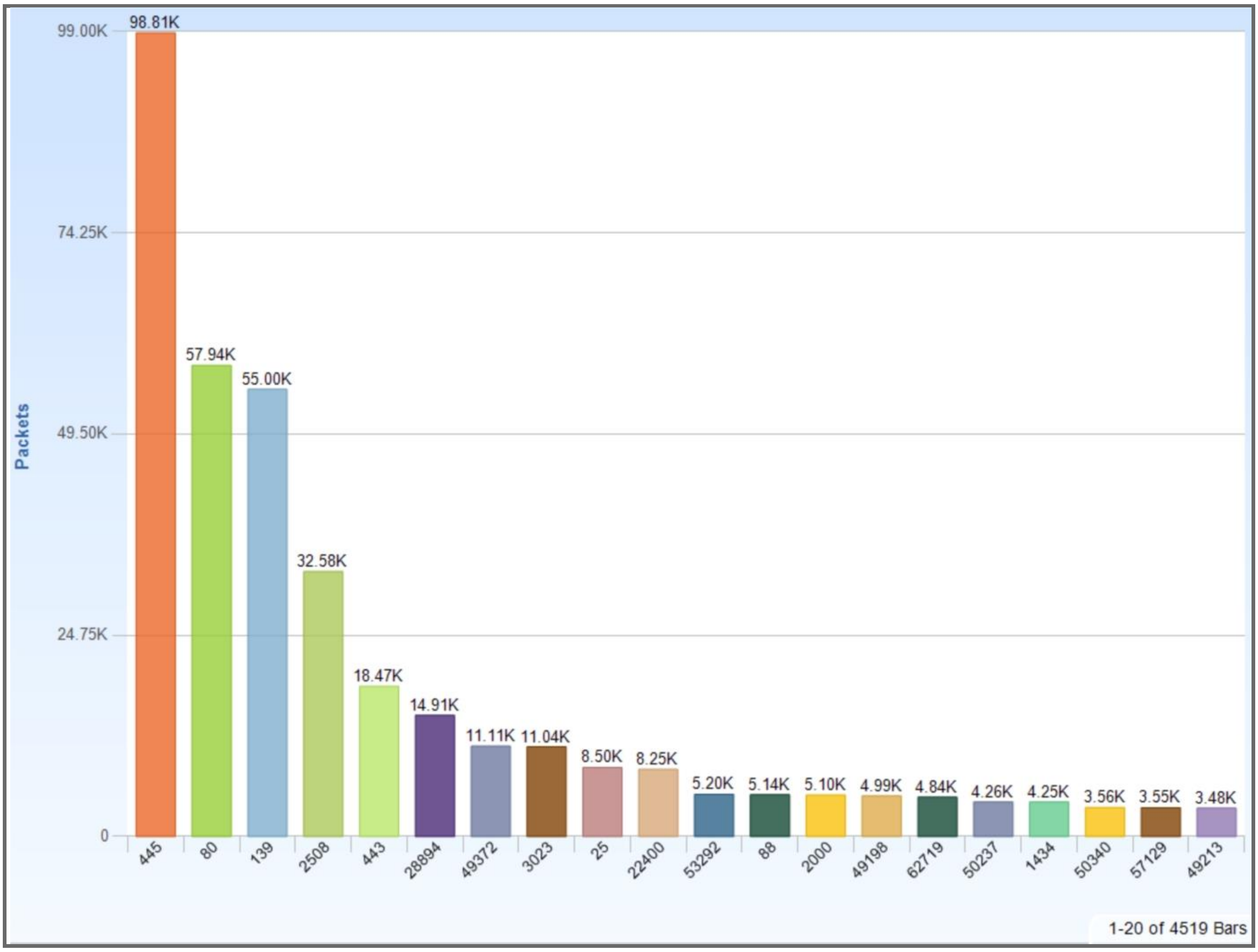


Figure 24 - TCP Packets

UDP Bytes

Top UDP source ports, ordered by total sent bytes.

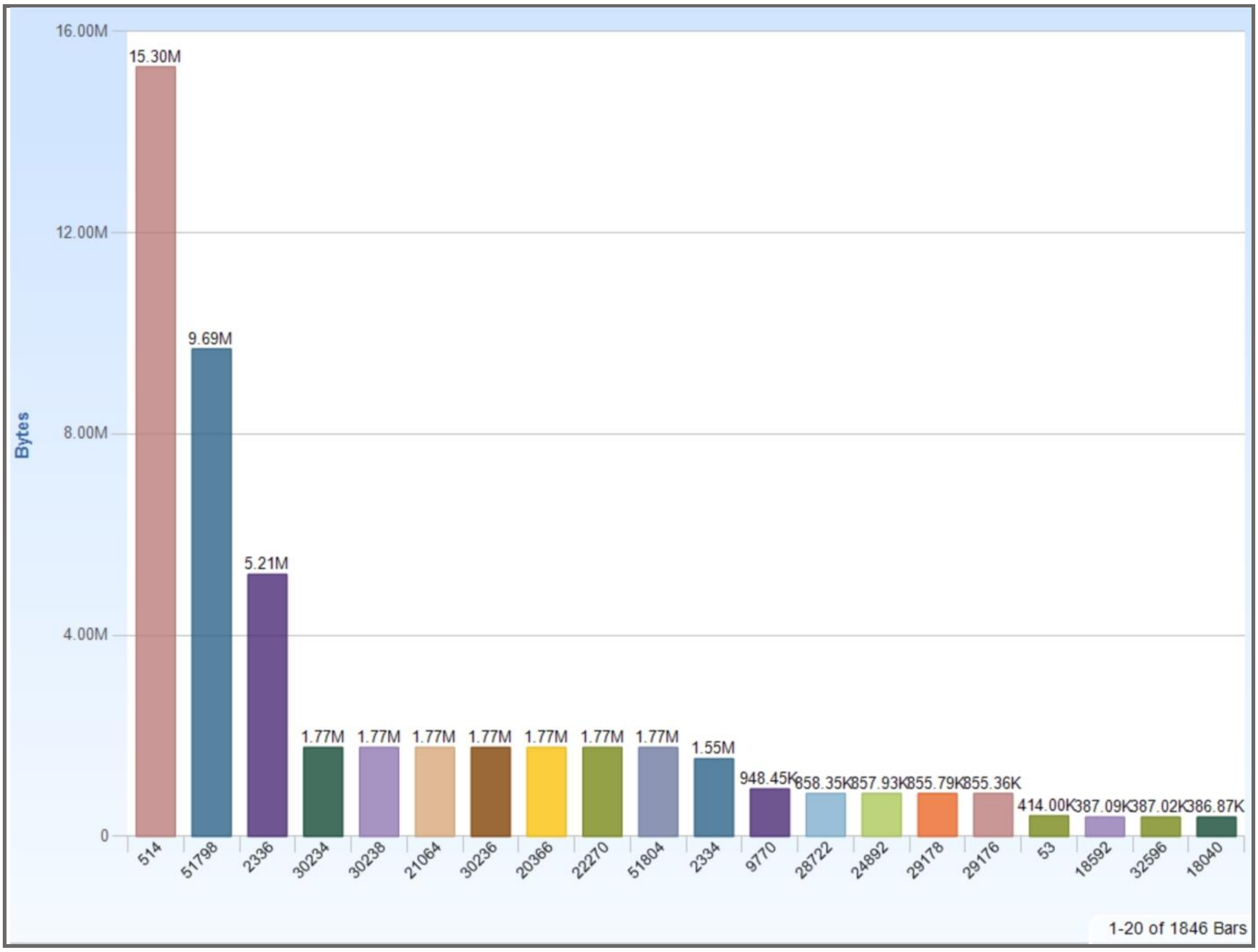


Figure 25 - UDP Bytes

UDP Bits

Top UDP source ports, ordered by total sent bits.

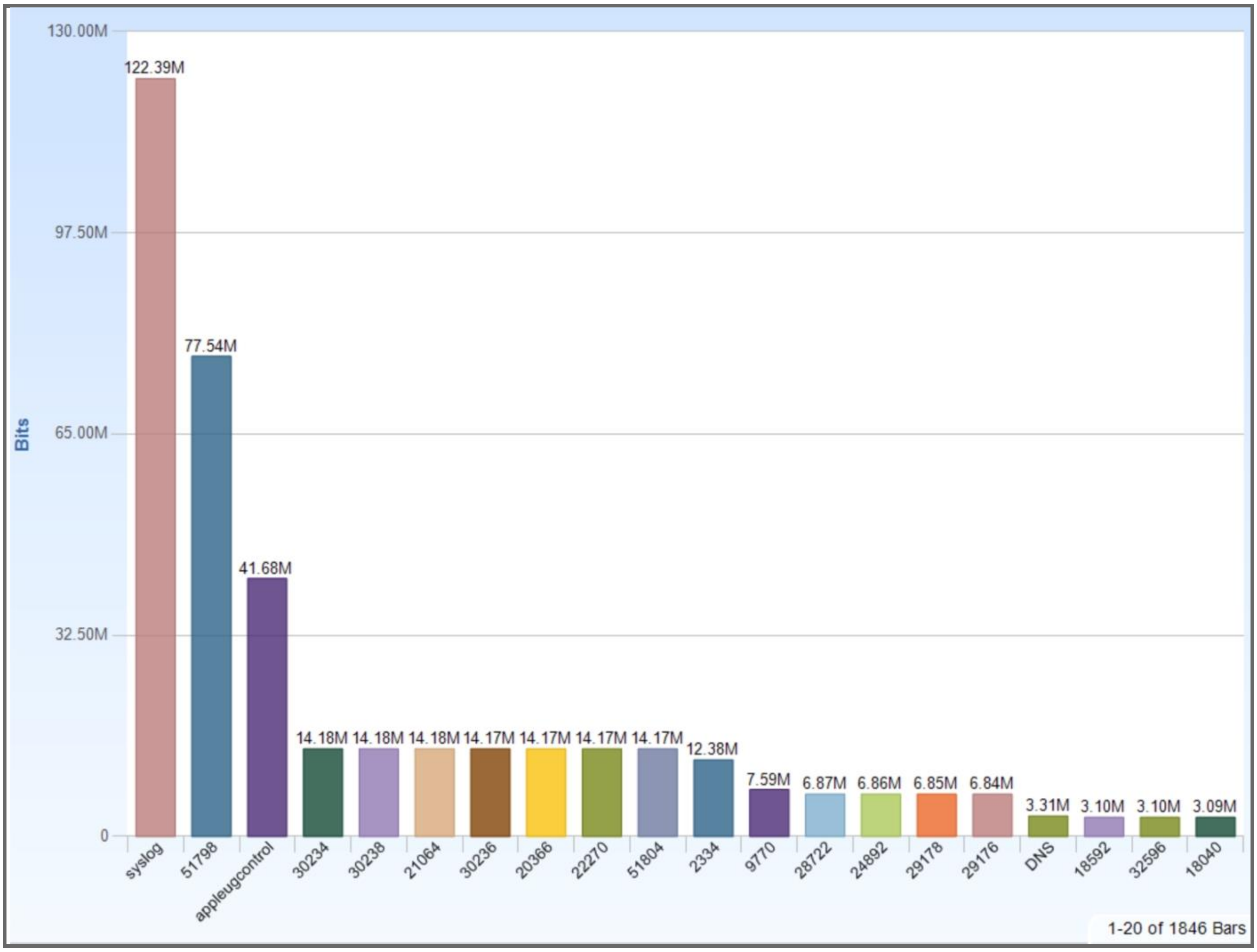


Figure 26 - UDP Bits

UDP Packets

Top UDP source ports, ordered by total sent packets.

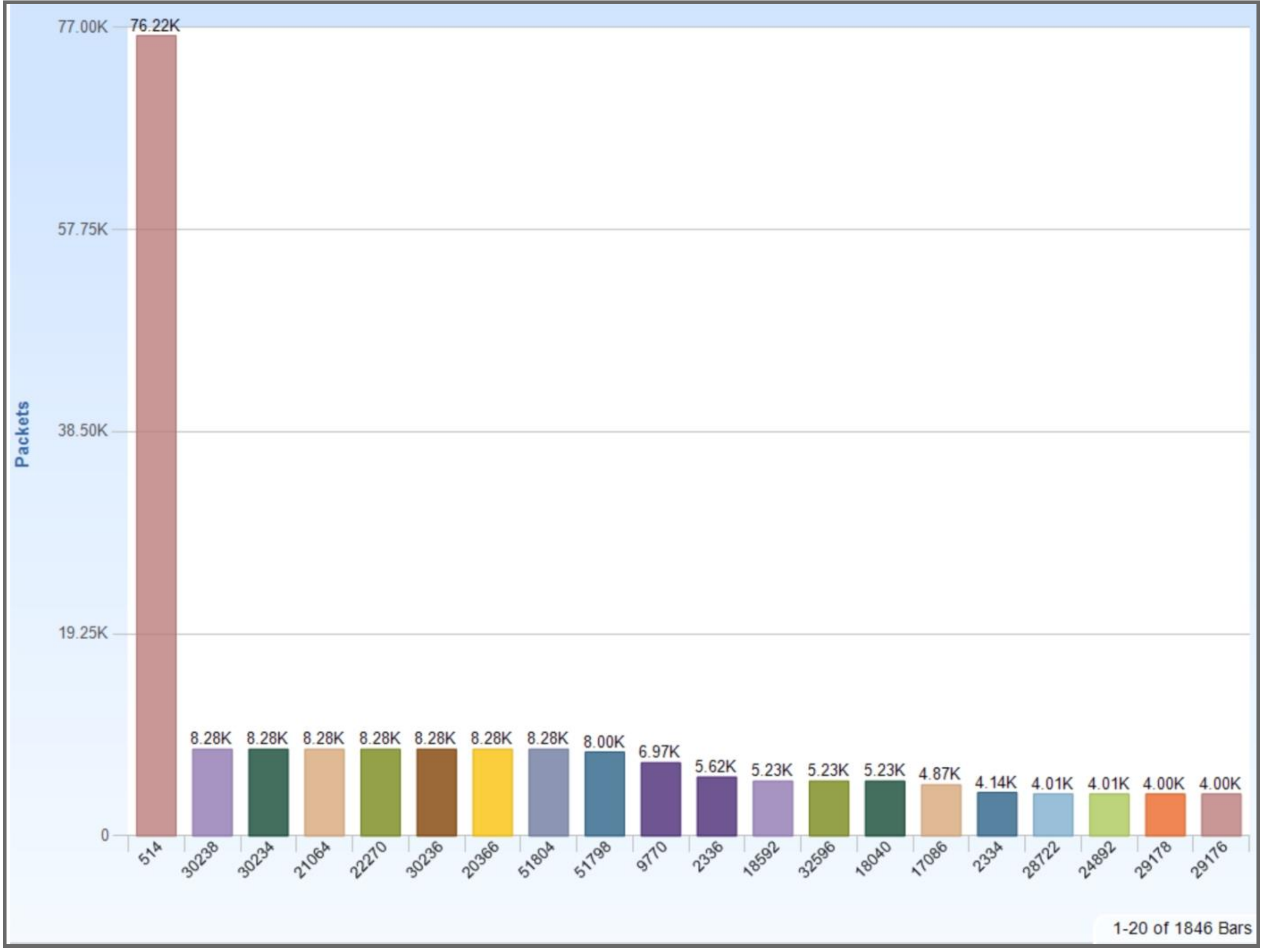


Figure 27 - UDP Packets

Top /24 Subnets

Top /24 IP subnets. Each entry in the charts includes the total traffic for the corresponding /24 IP subnet.

Top /24 Subnets - Packets

Each bar reports the total amount of packets sent or received by the corresponding IP subnet. The bar value is broken down into three categories: received packets (i.e. packets that come from a different subnet), sent packets (i.e. packets that leave the subnet), and internal packets (i.e. packets that are sent and received inside the subnet).

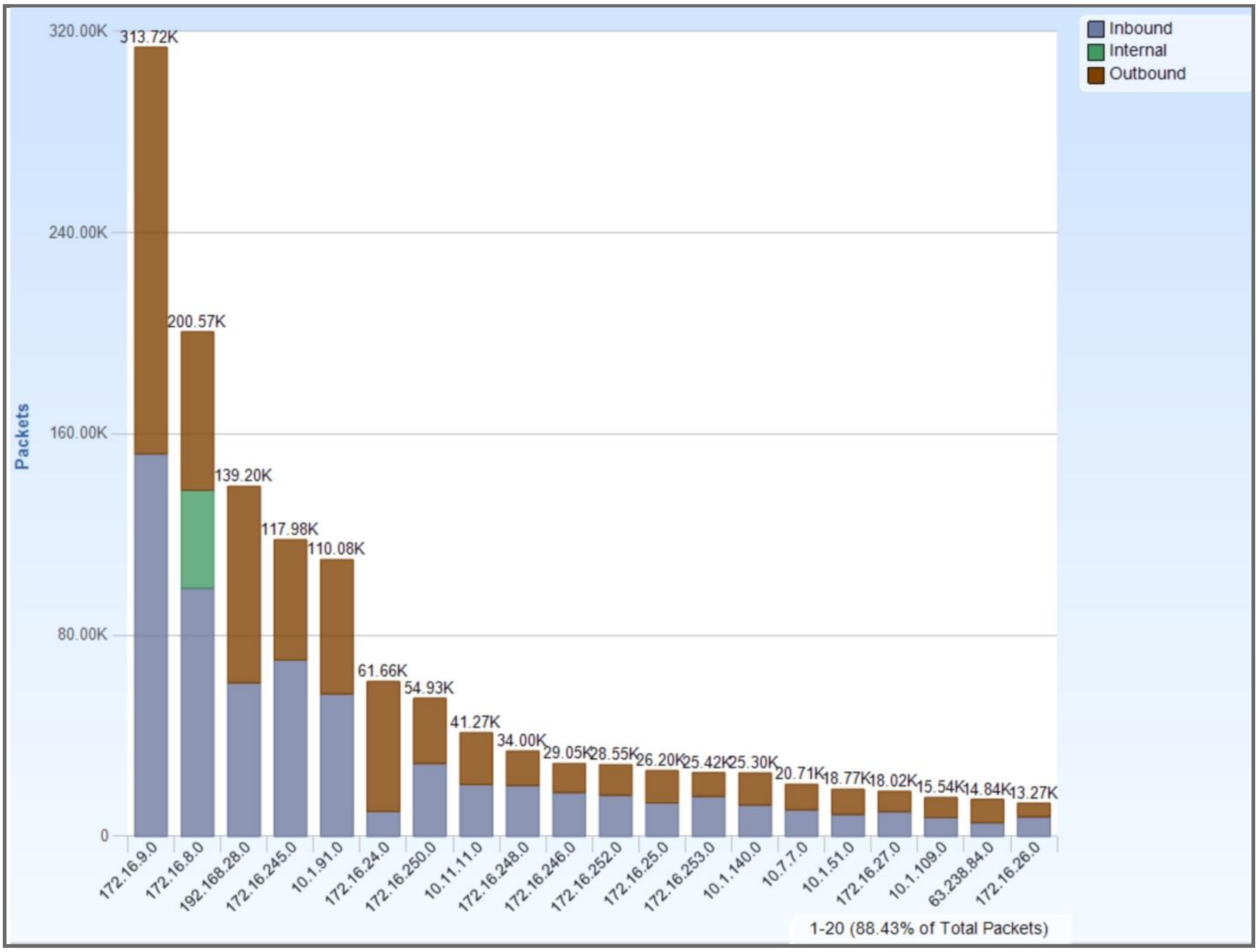


Figure 28 - Top /24 Subnets - Packets

Top /24 Subnets - Bytes

Each bar reports the total amount of bytes sent or received by the corresponding IP subnet. The bar value is broken down into three categories: received bytes (i.e. bytes that come from a different subnet), sent bytes (i.e. bytes that leave the subnet), and internal bytes (i.e. bytes that are sent and received inside the subnet).

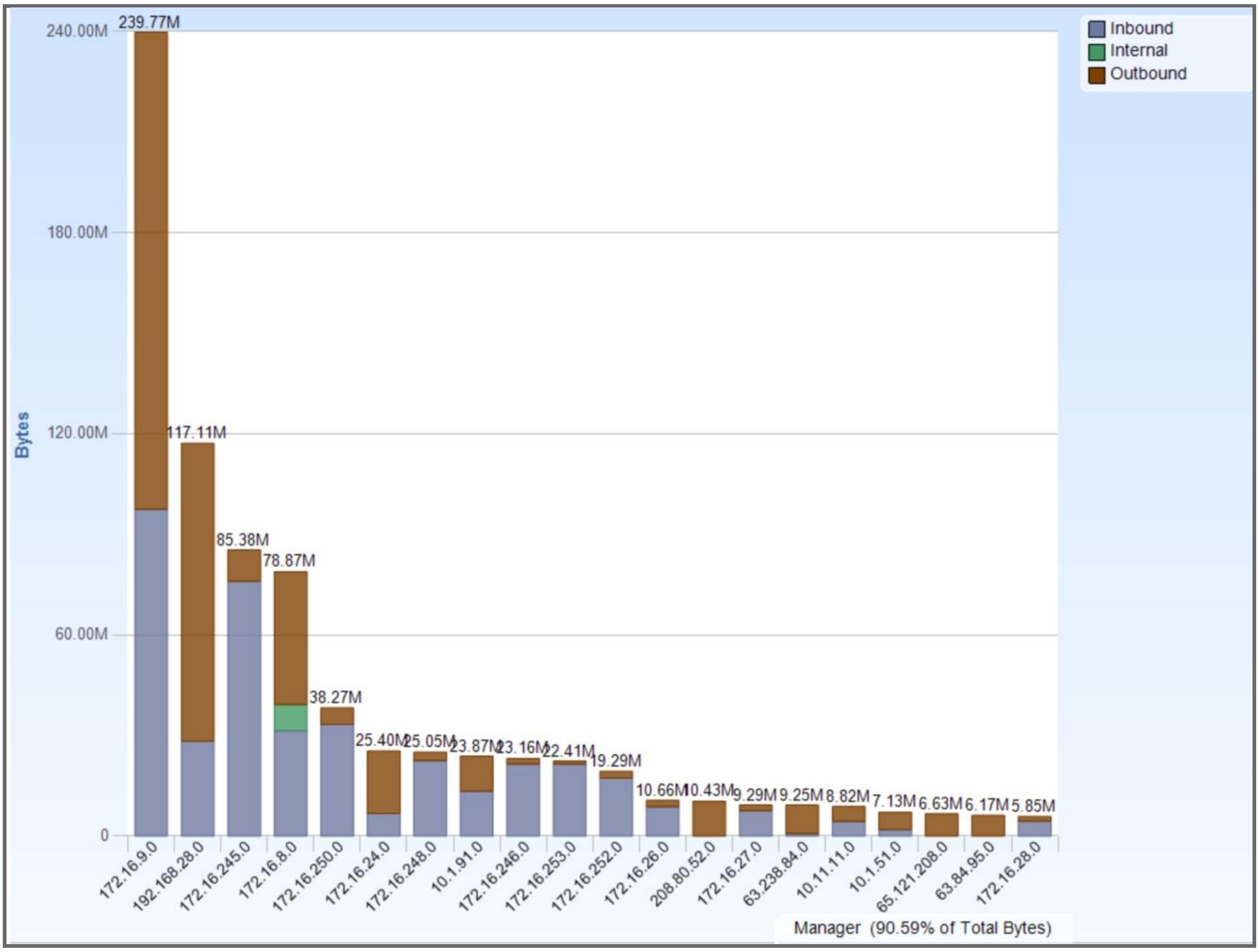


Figure 29 - Top /24 Subnets - Bytes

Top /24 Subnets - Bits

Each bar reports the total amount of bits sent or received by the corresponding IP subnet. The bar value is broken down into three categories: received bits (i.e. bits that come from a different subnet), sent bits (i.e. bits that leave the subnet), and internal bits (i.e. bits that are sent and received inside the subnet).

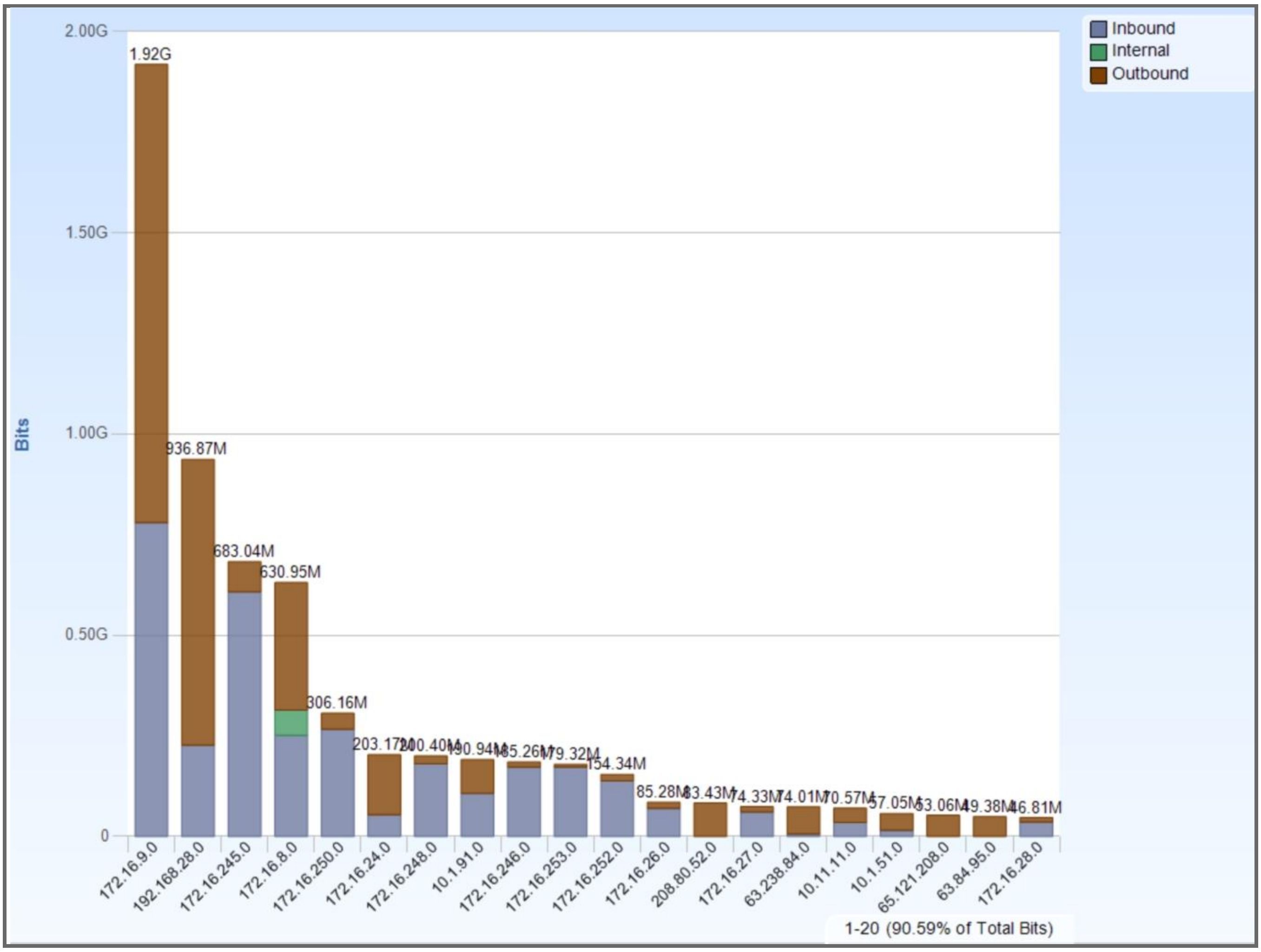


Figure 30 - Top /24 Subnets - Bits

Top /8 Subnets

Top /8 IP subnets. Each entry in the charts includes the total traffic for the corresponding /8 IP subnet.

Top /8 Subnets - Packets

Each bar reports the total amount of packets sent or received by the corresponding IP subnet. The bar value is broken down into three categories: received packets (i.e. packets that come from a different subnet), sent packets (i.e. packets that leave the subnet), and internal packets (i.e. packets that are sent and received inside the subnet).

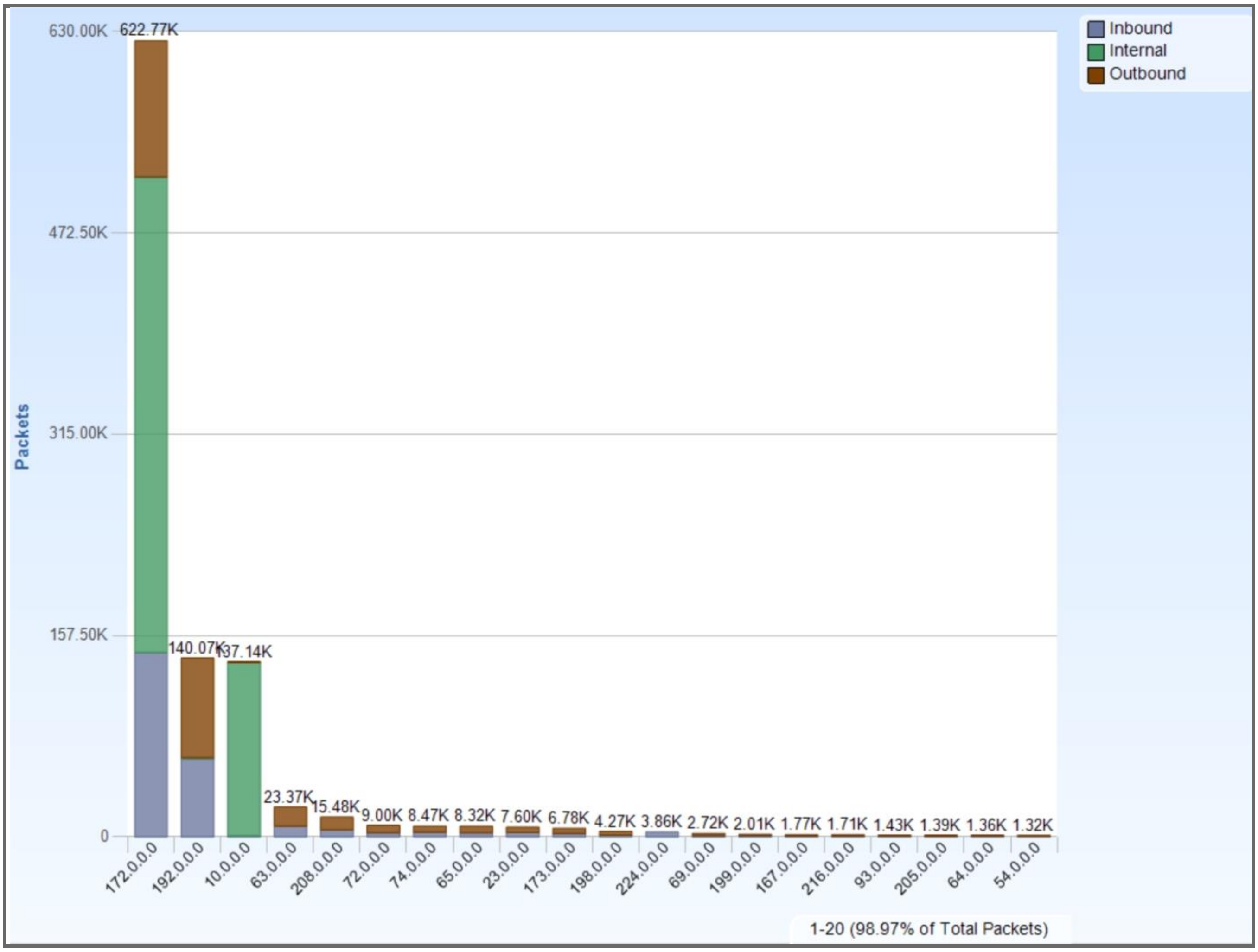


Figure 31 - Top /8 Subnets - Packets

Top /8 Subnets - Bytes

Each bar reports the total amount of bytes sent or received by the corresponding IP subnet. The bar value is broken down into three categories: received bytes (i.e. bytes that come from a different subnet), sent bytes (i.e. bytes that leave the subnet), and internal bytes (i.e. bytes that are sent and received inside the subnet).

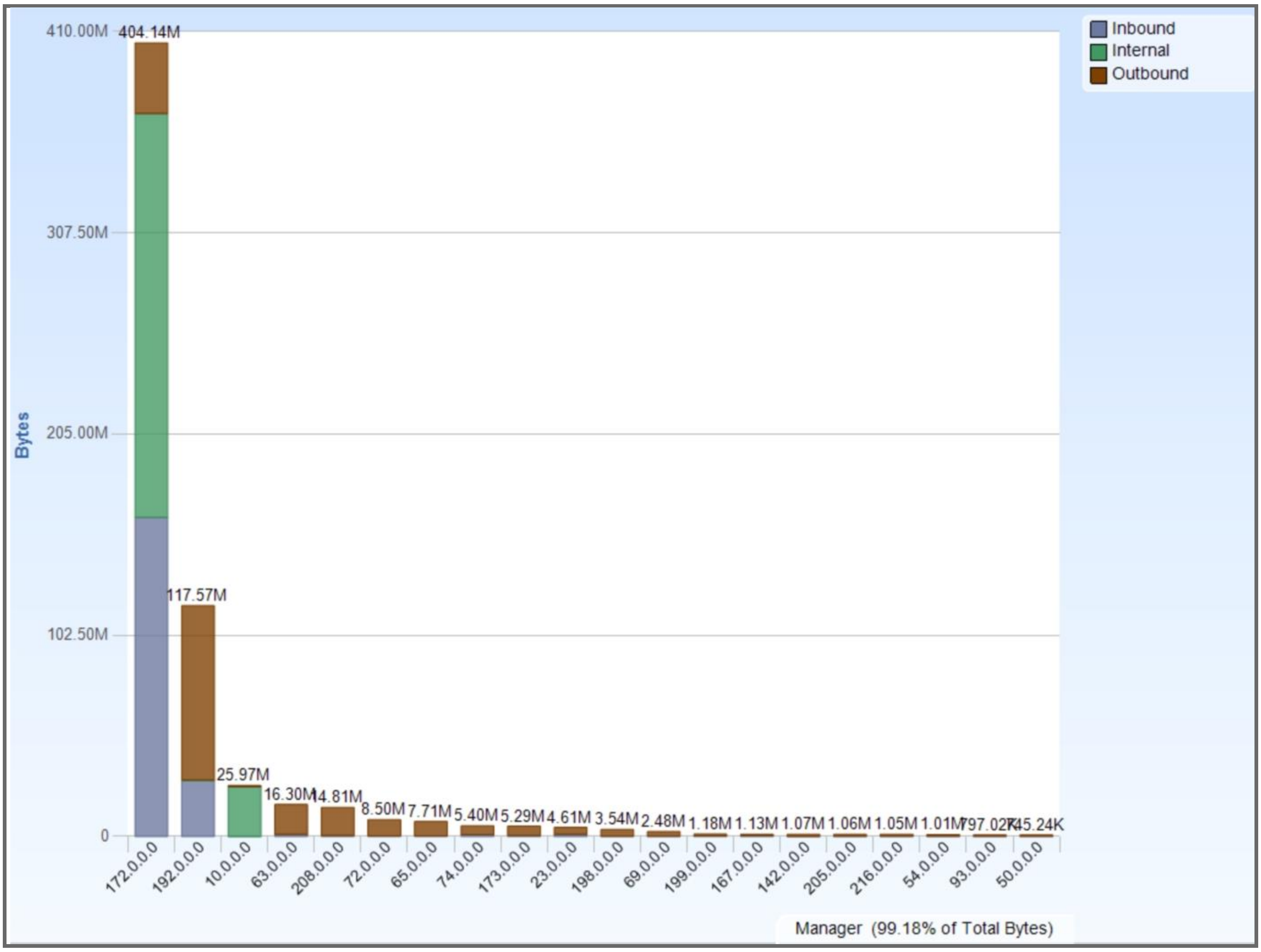


Figure 32 - Top /8 Subnets - Bytes

Top /8 Subnets - Bits

Each bar reports the total amount of bits sent or received by the corresponding IP subnet. The bar value is broken down into three categories: received bits (i.e. bits that come from a different subnet), sent bits (i.e. bits that leave the subnet), and internal bits (i.e. bits that are sent and received inside the subnet).

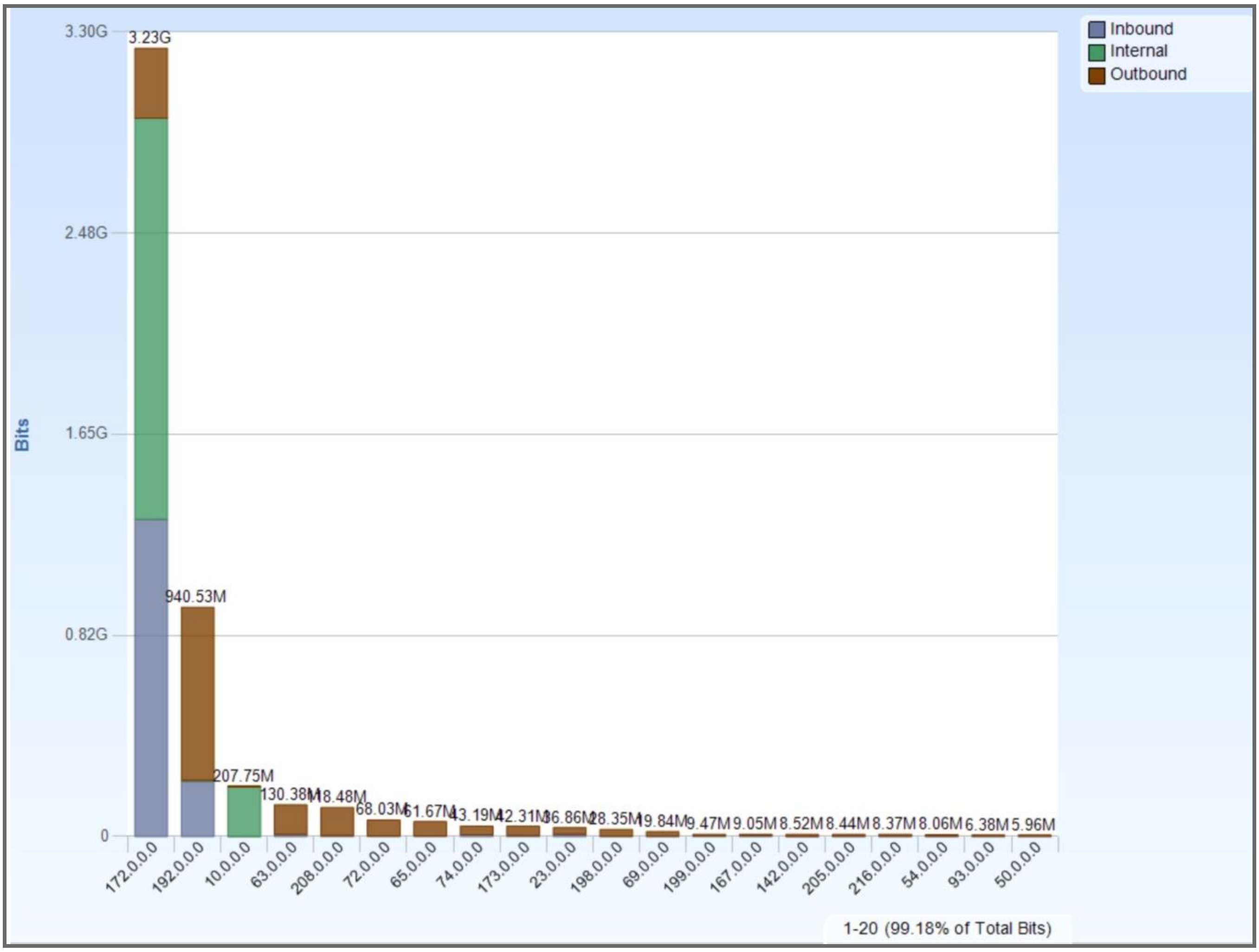


Figure 33 - Top /8 Subnets - Bits

VoIP Conversations by IP

VoIP Conversations among IP hosts

IP Conversations

VoIP host conversations. The size of the host is relative to the amount of signaling and data (RTP) it has transmitted. The size of each connection is relative to how much VoIP traffic is transported between the two endpoints.

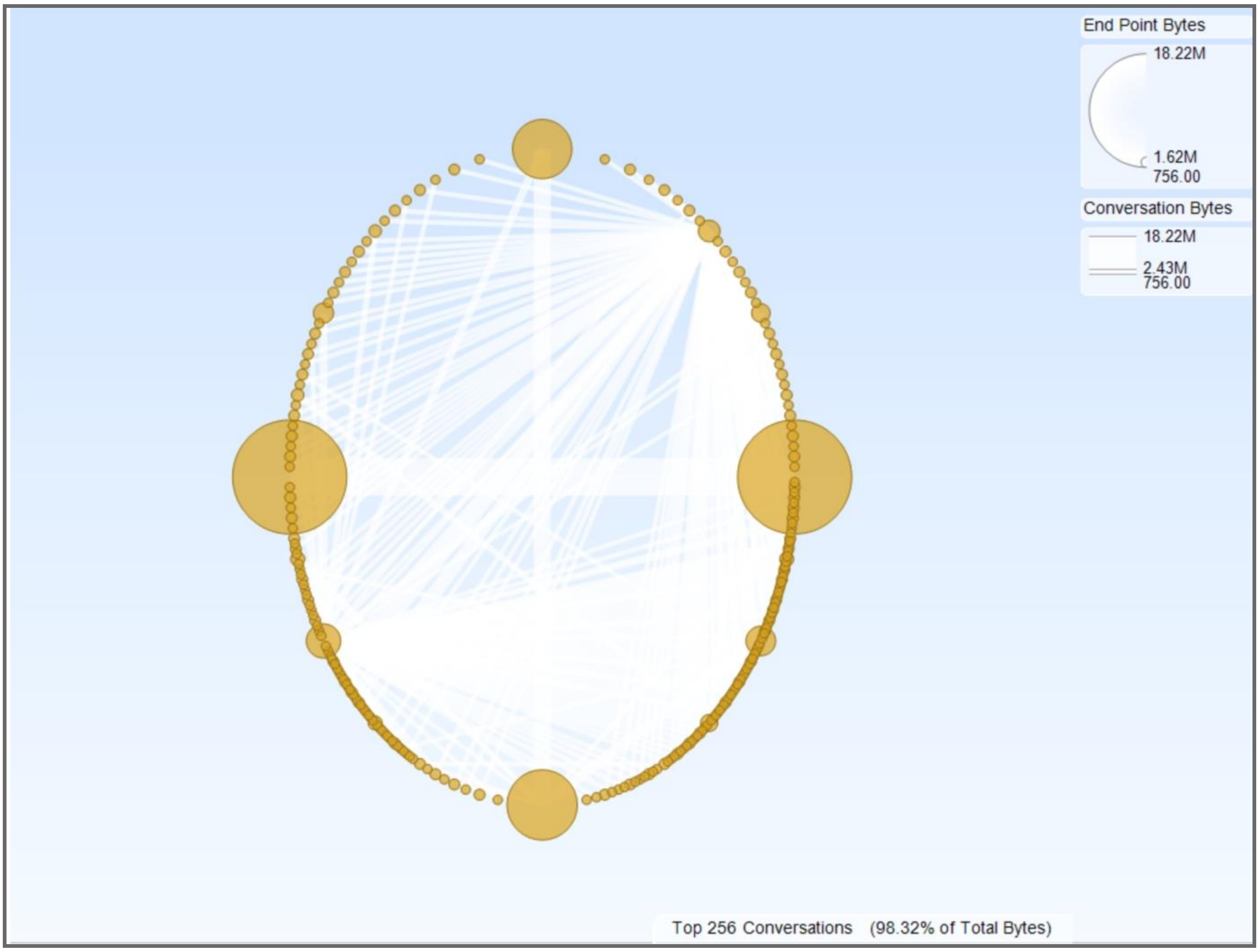


Figure 34 - IP Conversations

VoIP Failed Calls - Top IP Talkers

Top IP Talkers for failed VoIP Calls

Top IP Sources for Failed Calls

Top IP sources for failed VoIP calls.

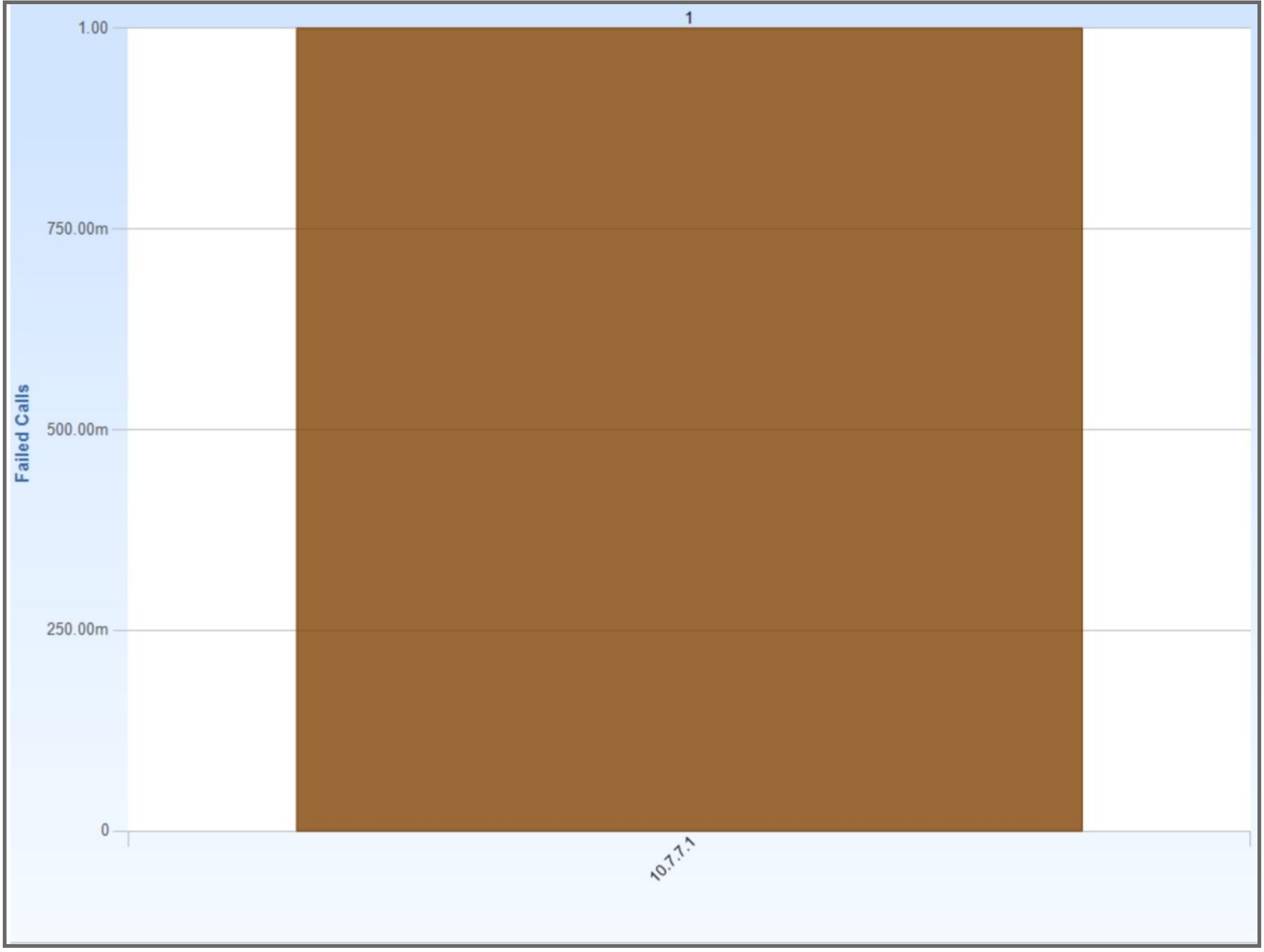


Figure 35 - Top IP Sources for Failed Calls

Top IP Destinations for Failed Calls

Top IP destinations for failed VoIP calls.

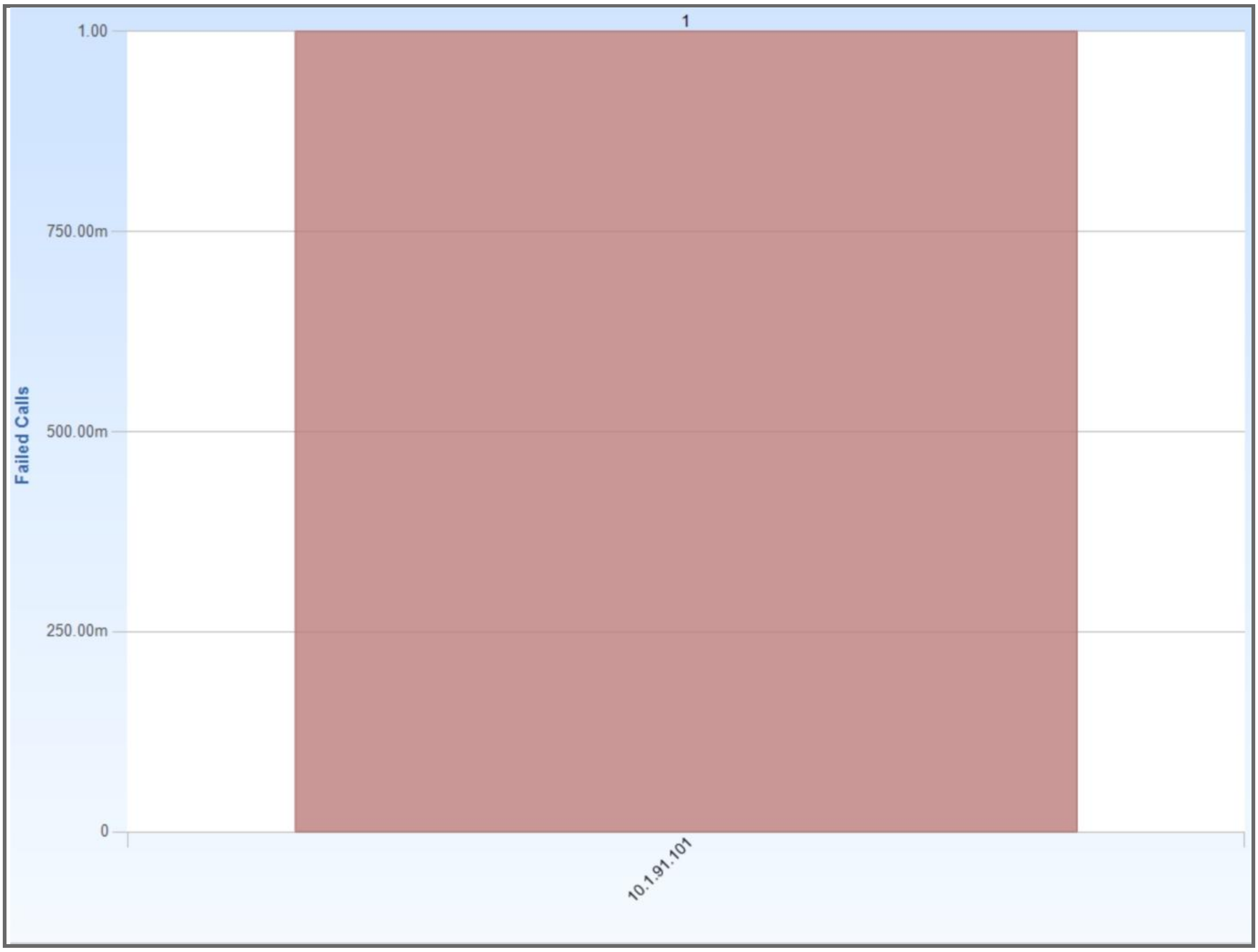


Figure 36 - Top IP Destinations for Failed Calls

Top IP Talkers for Failed Calls

Top IP talkers for failed VoIP calls.

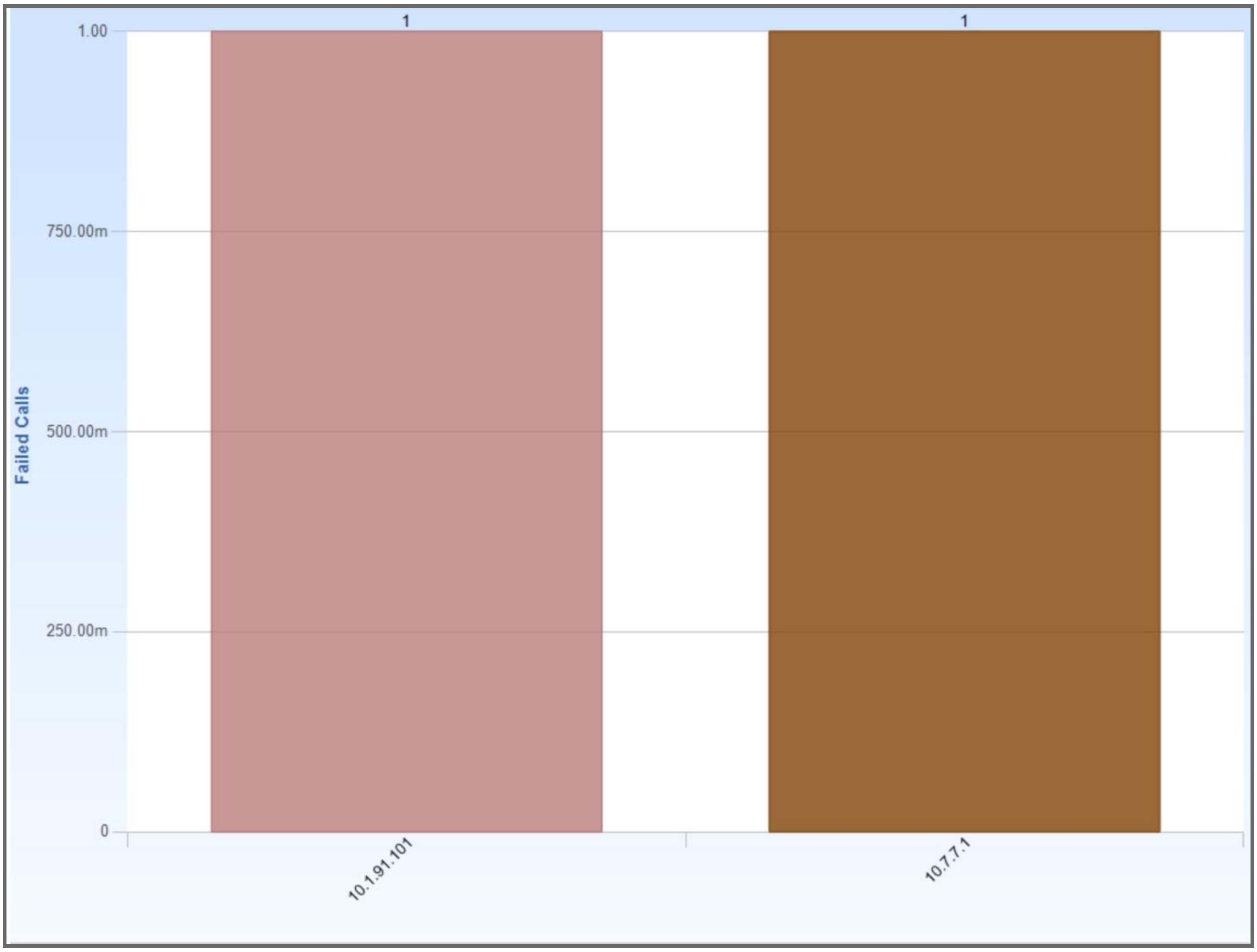


Figure 37 - Top IP Talkers for Failed Calls

TCP Bandwidth Over Time by Direction

TCP Bandwidth Over Time by Direction

TCP Server to Client Bytes Per Seconds

TCP server to client bandwidth (bytes per seconds).

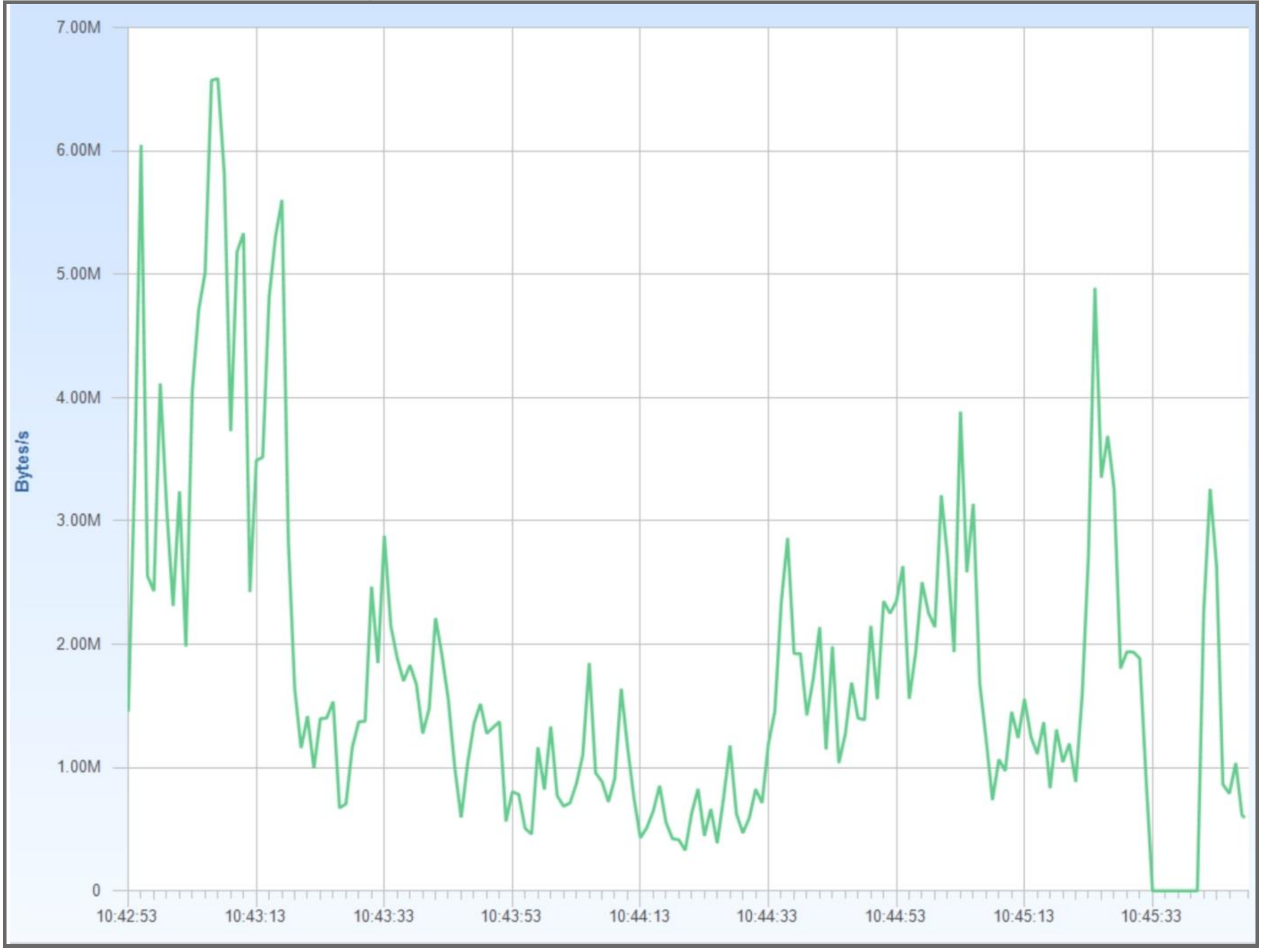


Figure 38 - TCP Server to Client Bytes Per Seconds

TCP Server to Client Bits Per Seconds

TCP server to client bandwidth (bits per seconds).

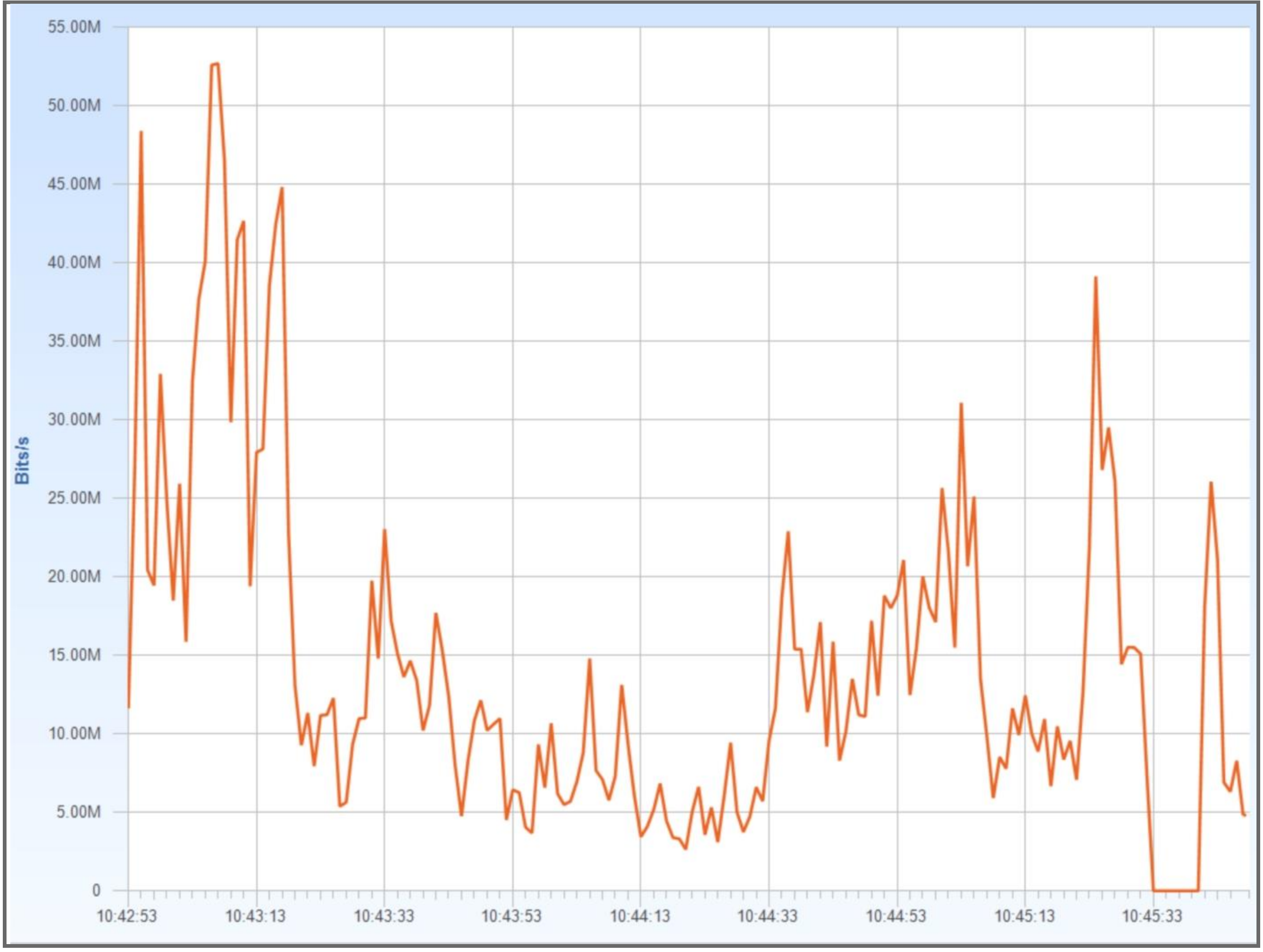


Figure 39 - TCP Server to Client Bits Per Seconds

TCP Server to Client Packets Per Seconds

TCP server to client bandwidth (packets per seconds).

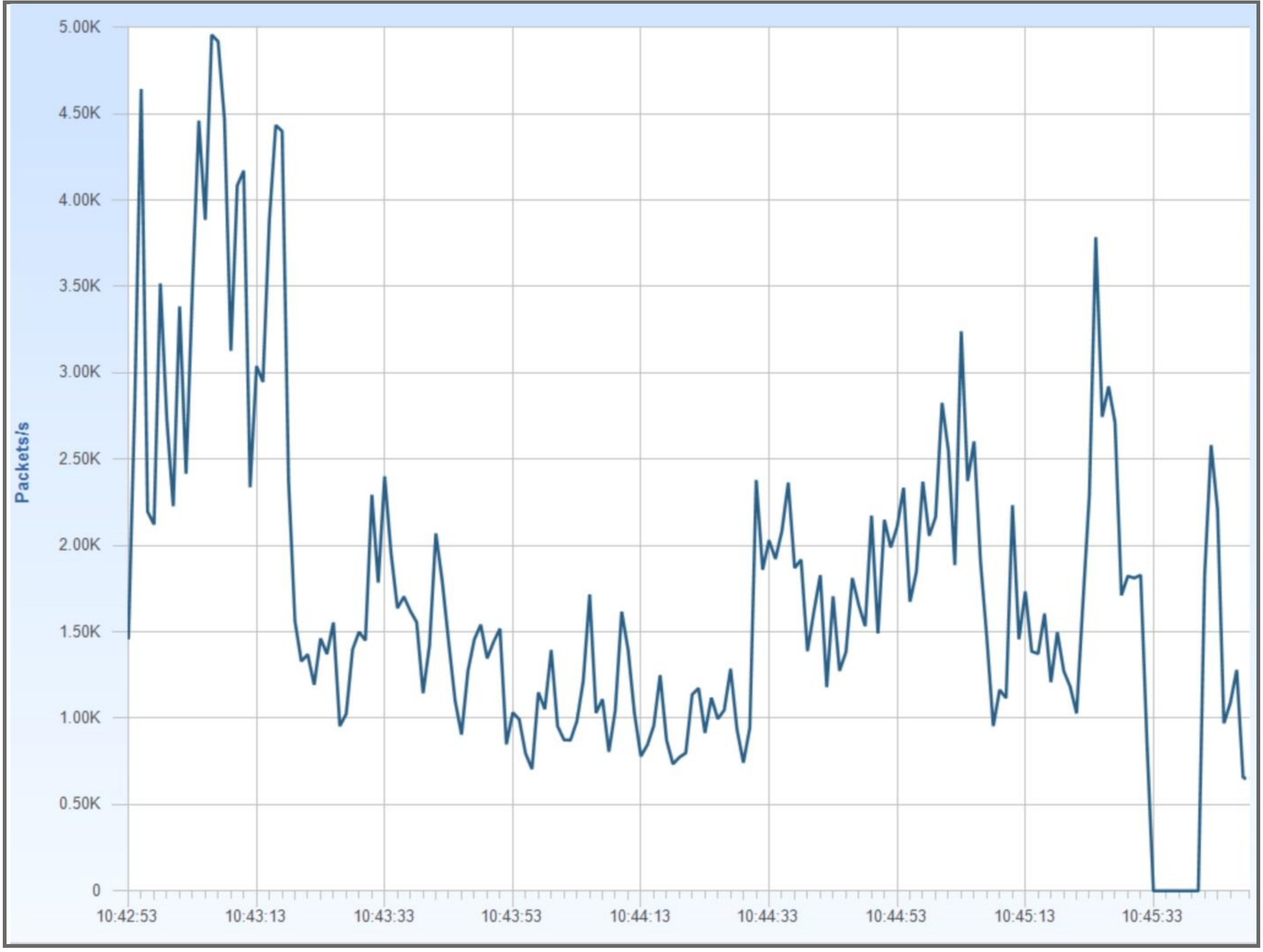


Figure 40 - TCP Server to Client Packets Per Seconds

TCP Client To Server Bytes Per Seconds

TCP client to server bandwidth (bytes per seconds).

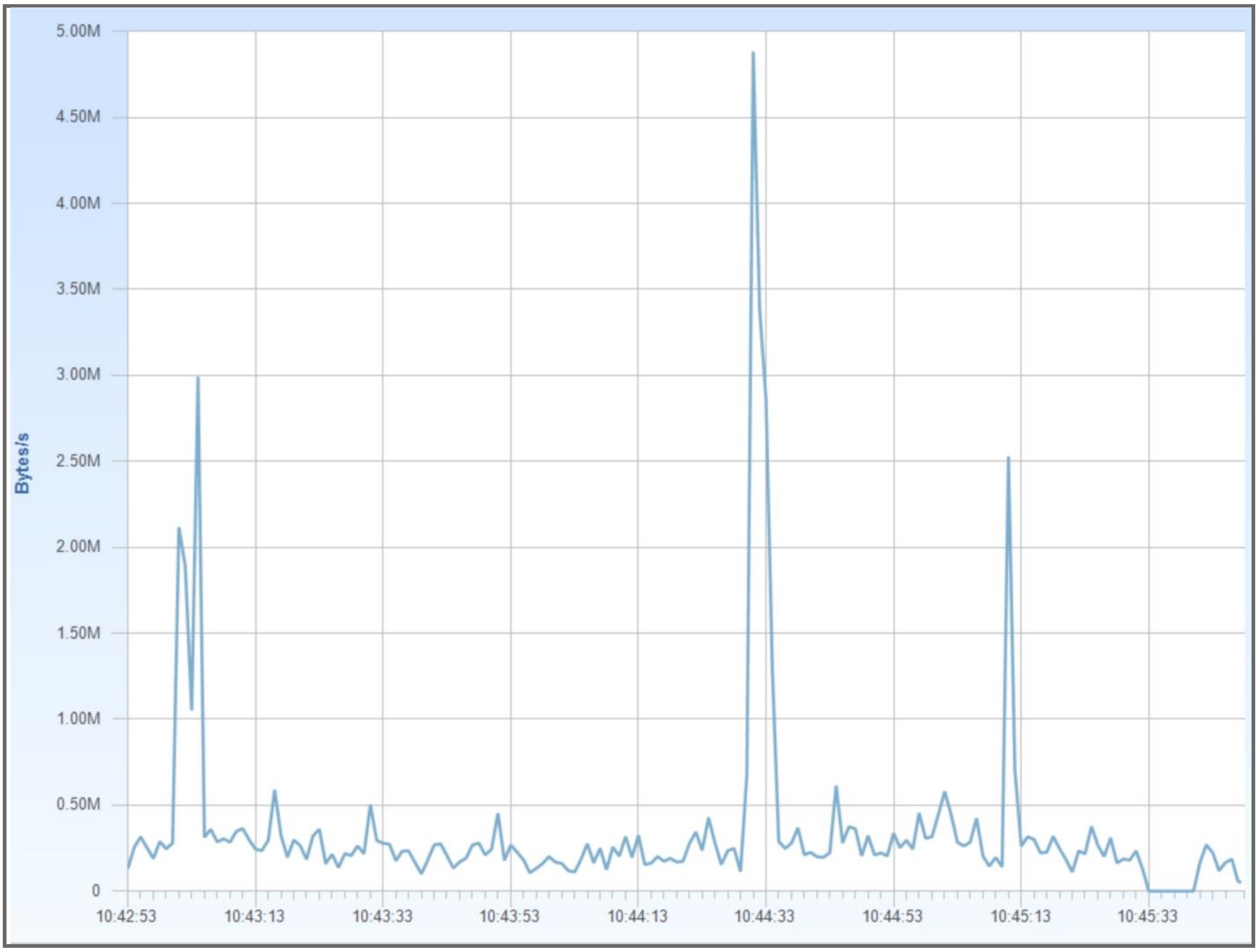


Figure 41 - TCP Client To Server Bytes Per Seconds

TCP Client To Server Bits Per Seconds

TCP client to server bandwidth (bits per seconds).

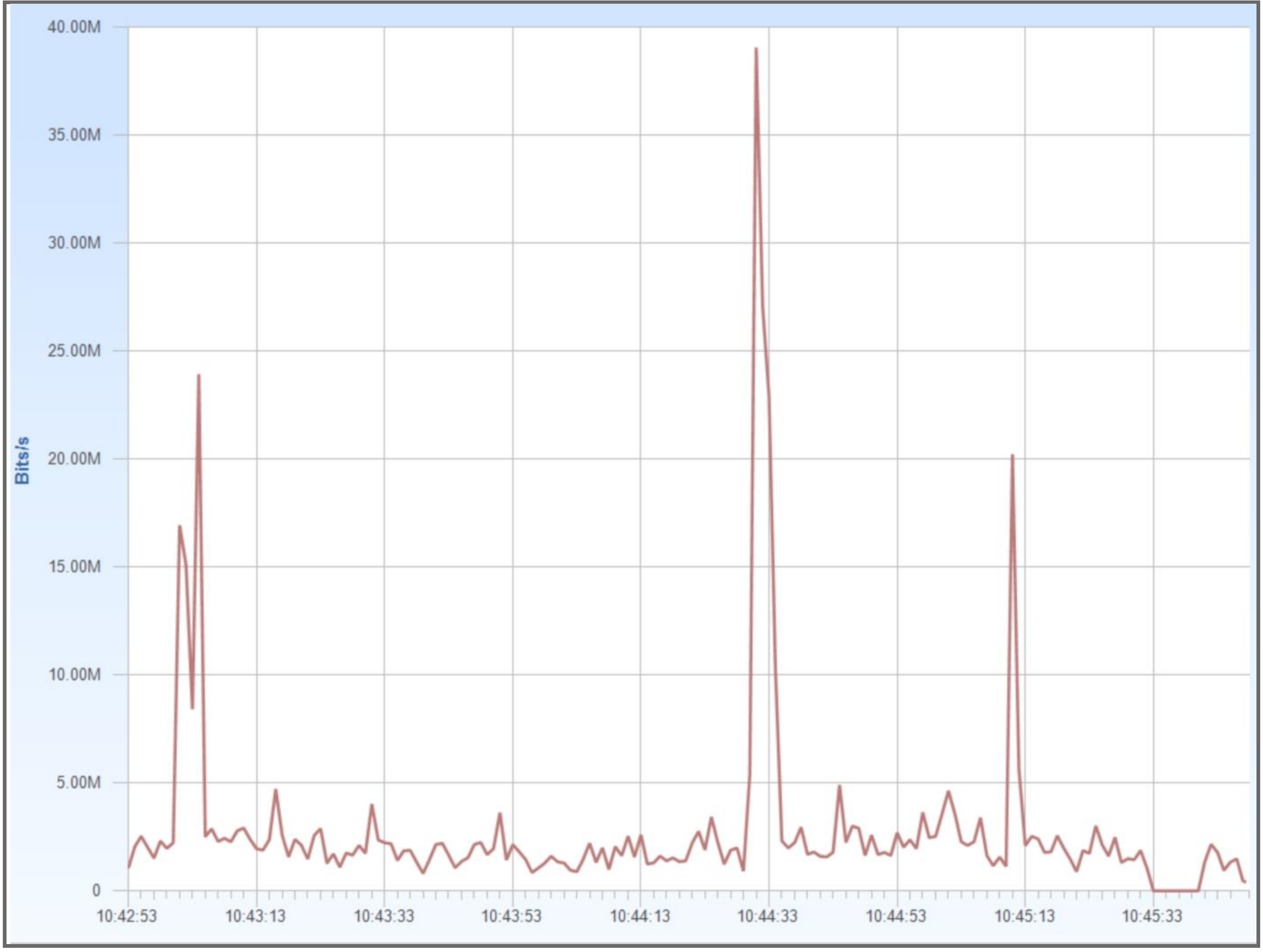


Figure 42 - TCP Client To Server Bits Per Seconds

TCP Client To Server Packets Per Seconds

TCP client to server bandwidth (packets per seconds).

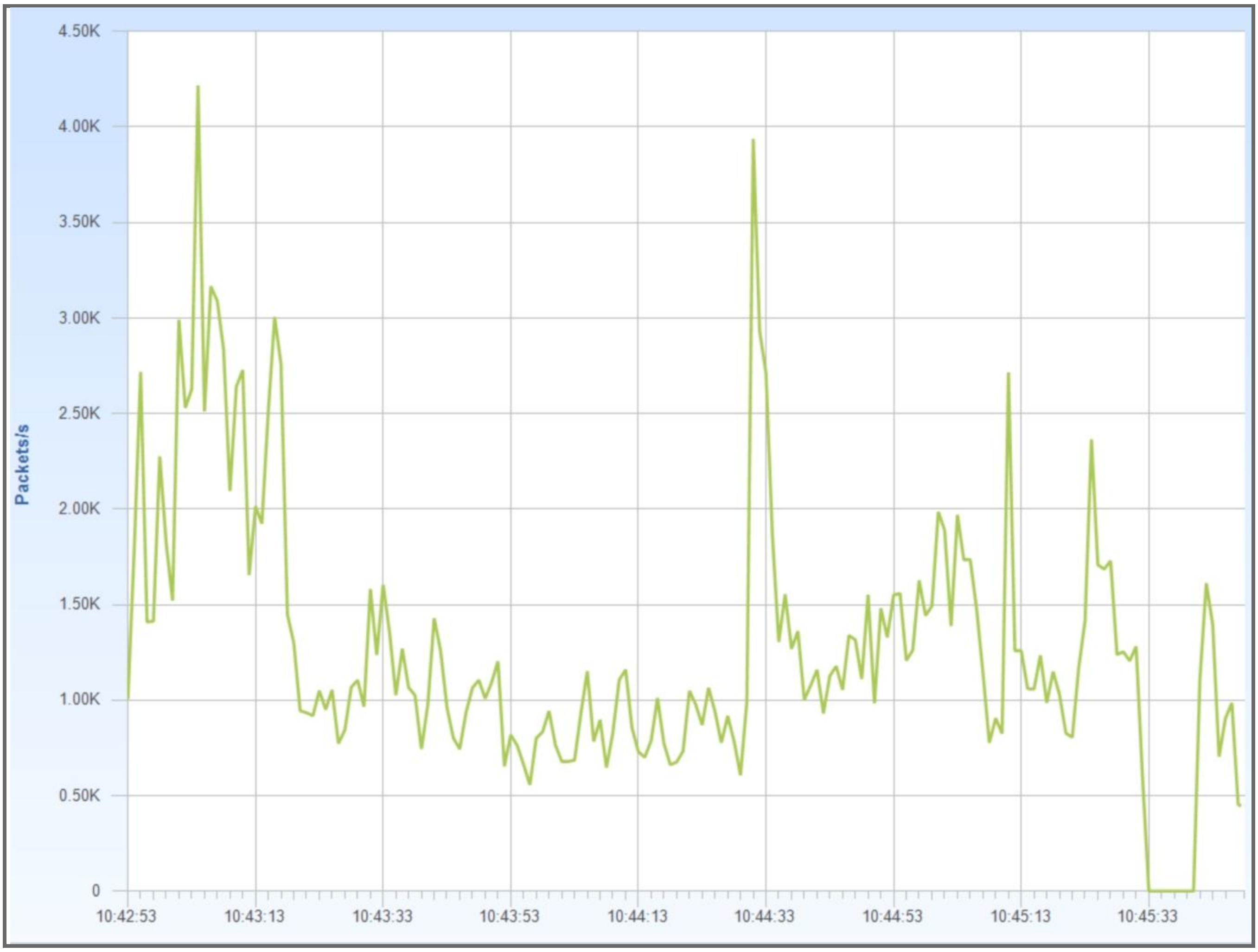


Figure 43 - TCP Client To Server Packets Per Seconds

TCP vs. UDP Bandwidth

Overview of TCP and UDP traffic (ports and protocols)

TCP/UDP Bits

Bandwidth in bytes per second used by the TCP and UDP protocols.

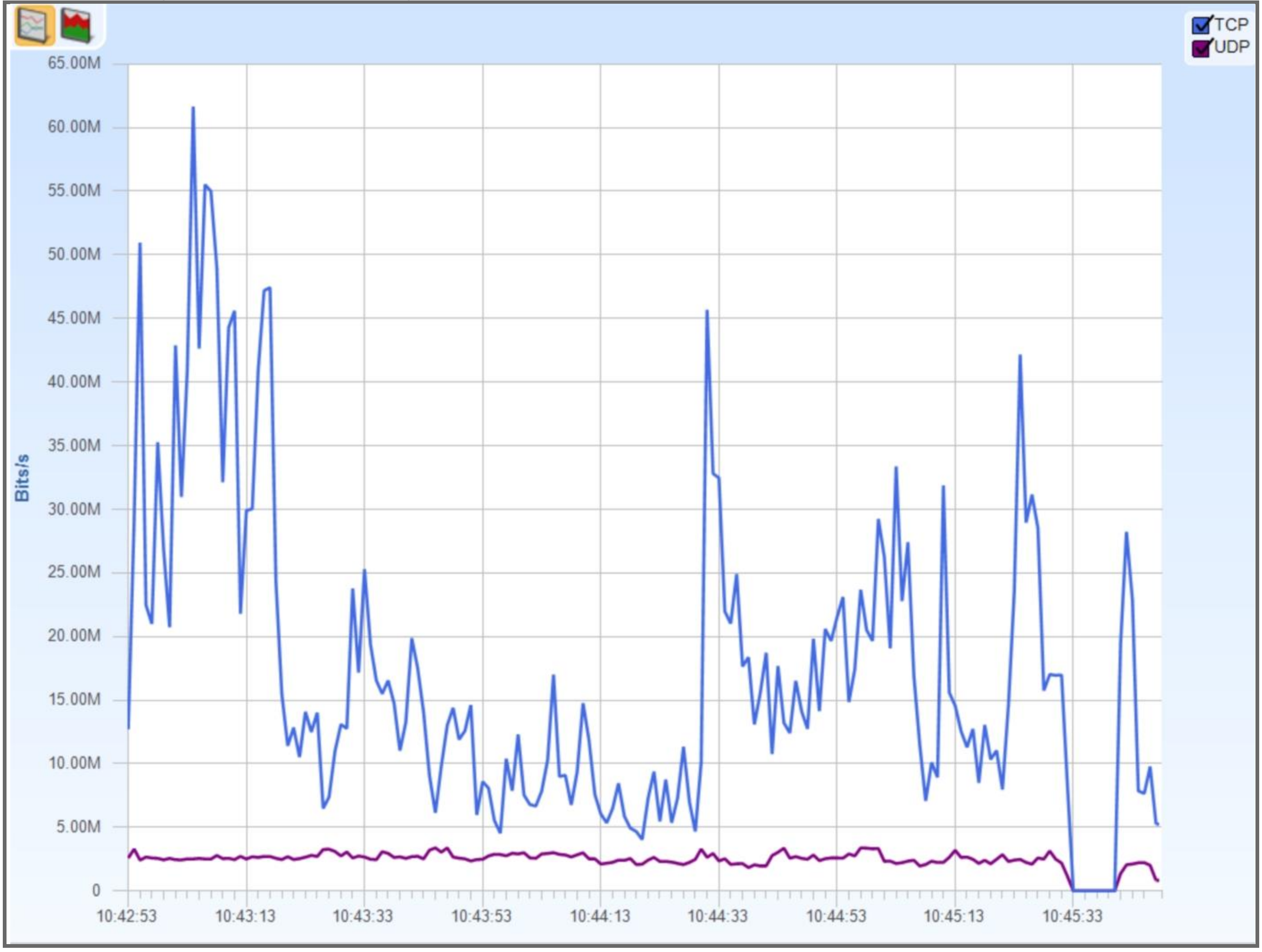


Figure 44 - TCP/UDP Bits

Traffic By Ports - TCP

TCP traffic by port.

Data

Protocol	Port	Total Bits	Total Packets
microsoft-ds	445	920,820,584	162,421
netbios-ssn	139	597,229,128	87,939
http	80	588,260,192	96,138
Unknown	0	242,900,720	86,974
smtp	25	188,772,896	25,986

Protocol	Port	Total Bits	Total Packets
https	443	134,328,432	30,654
ms-sql-m	1434	41,588,360	7,052
sip-tls	5061	16,539,032	3,221
kerberos	88	9,735,832	5,151
ldap	389	9,514,736	4,054
ms-sql-s	1433	8,659,768	3,317
ssh	22	5,158,104	1,042
ftp-data	20	4,849,568	620
SCCP	2000	1,227,360	12,289
epmap	135	263,040	208
ms-rdp-server	3389	185,392	2,482
h323hostcall	1720	130,424	352
http-alt	8080	63,920	344
sql*net2	1521	30,840	14
sip	5060	22,728	36
ftp	21	4,344	30
macromedia-fcs	1935	832	24
jabber-client	5222	24	6
echo	7	0	119

Traffic By Ports - UDP

UDP traffic by port.

Data

rtp	51798	114,646,464	13,614
syslog	514	96,789,160	76,228
rtp	30234	22,787,936	16,561
rtp	30238	22,786,560	16,560
rtp	30236	22,783,808	16,558
rtp	51804	22,380,960	12,415
rtp	29178	11,021,760	8,010
rtp	29176	11,016,256	8,006
Unknown	0	9,142,384	9,896
DNS	53	3,338,272	3,321
rtp	18592	2,677,504	10,459
rtp	32596	2,514,432	10,099
rtp	29476	2,385,632	1,741
rtp	19376	1,982,464	7,744
snmp	161	1,678,296	545
netbios-dgm	138	1,563,248	1,009
rtp	26606	1,384,704	5,409

rtp	19224	778,336	572
rtp	28996	670,976	2,621
rtp	29468	587,552	427
netbios-ns	137	320,840	593
ldap	389	71,392	45
ntp	123	64,512	168
ssdp	1900	11,904	12
mgcp-gateway	2427	10,672	44
dhcp	67	9,600	4
sip	5060	8,824	2
rtp	25926	6,144	24
ms-sql-m	1434	4,208	10