PROFITAP

IOTA

APPLICATION LATENCY ANALYSIS

VISIT WWW.PROFITAP.COM

Problem Description

More and more applications are provided by cloud providers as SaaS from globally distributed data centers. Normally, this offers easy application deployment. However, it also brings new error sources that can affect application performance. For example, latency issues can lead to sluggish applications and even timeouts in those applications. With packet loss, similar behavior occurs, and retransmissions are visible.

Real-time applications, particularly video conferencing via Microsoft Teams or WebEx, react very sensitively to such error patterns. High latencies also negatively affect application performance in legacy applications with direct sequential database queries over a WAN link.

If applications freeze up, this is in many cases due to TCP Zero Windows. When this happens, the network has transmitted the user data correctly, but the server or client cannot process it further due to local performance limitations.

In addition, SD-WAN solutions with a combination of WAN links with different bandwidth, packet loss, and latency characteristics are increasingly being used. If, despite positive representations in the associated management solutions, application performance is not satisfactory, a familiar game quickly gets underway: finger-pointing between those responsible for the application, client, server, and network.

Profitap IOTA wants to counteract this by simplifying troubleshooting with intuitive dashboards and reliable traffic capture.

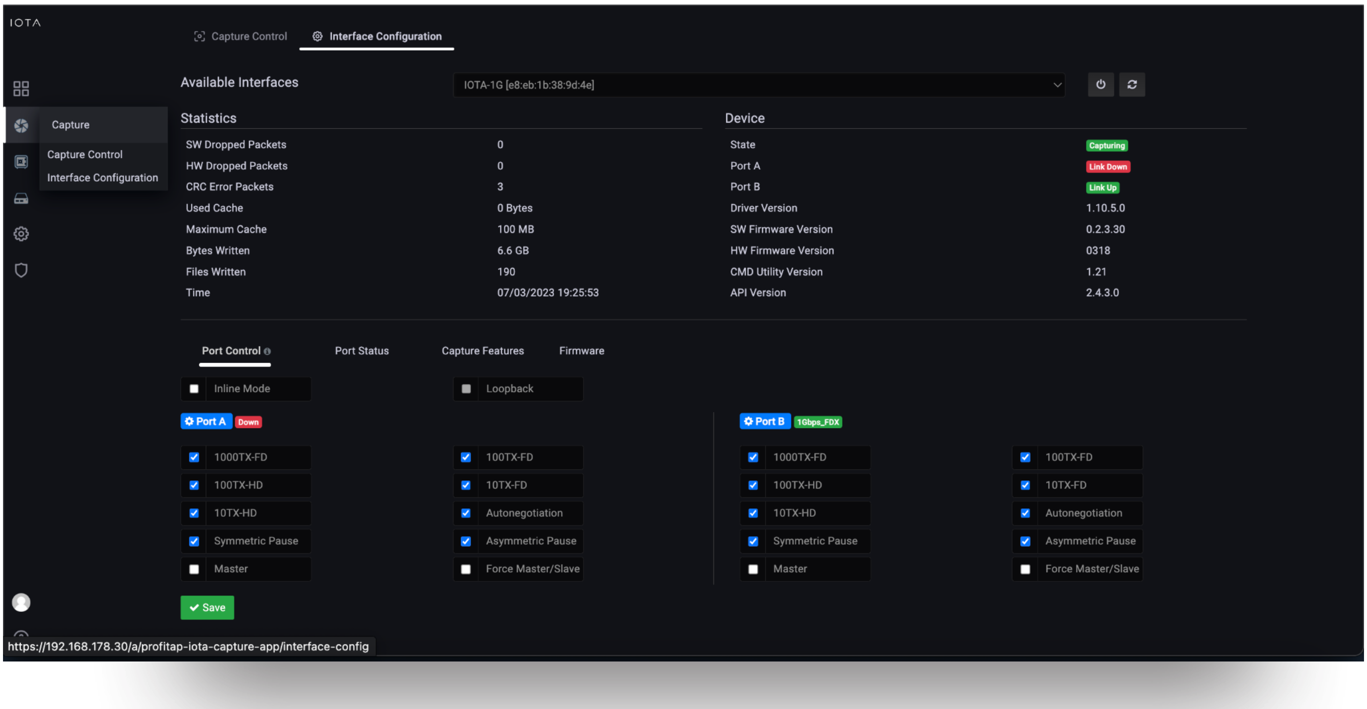
Troubleshooting Workflow

The following example gives a step-by-step overview of how an analysis of reduced application performance can be done with Profitap IOTA. The example used is a sluggish and freezing Office 365 application.

As the first step, we need to configure the physical interface. To do this, we navigate to the **Capture** menu in the left menu tree, and then to the **Interface Configuration** page.

In the configuration shown, the interface is configured in SPAN mode with 10/100/1000 Mbit/s Auto-Negotiation, so both physical interfaces can receive traffic to be analyzed from a SPAN port or a TAP.

If the IOTA is to be integrated inline in the data stream, the box next to **Inline Mode** must be checked and the **Save** button clicked.



Available Interfaces: IOTA-1G [e8:eb:1b:38:9d:4e]

Statistics

SW Dropped Packets	0
HW Dropped Packets	0
CRC Error Packets	3
Used Cache	0 Bytes
Maximum Cache	100 MB
Bytes Written	6.6 GB
Files Written	190
Time	07/03/2023 19:25:53

Device

State	Capturing
Port A	Link Down
Port B	Link Up
Driver Version	1.10.5.0
SW Firmware Version	0.2.3.30
HW Firmware Version	0318
CMD Utility Version	1.21
API Version	2.4.3.0

☐ Inline Mode ☐ Loopback

Port A Down

☑ 1000TX-FD ☑ 100TX-FD
☑ 100TX-HD ☑ 10TX-FD
☑ 10TX-HD ☑ Autonegotiation
☑ Symmetric Pause ☑ Asymmetric Pause
☐ Master ☐ Force Master/Slave

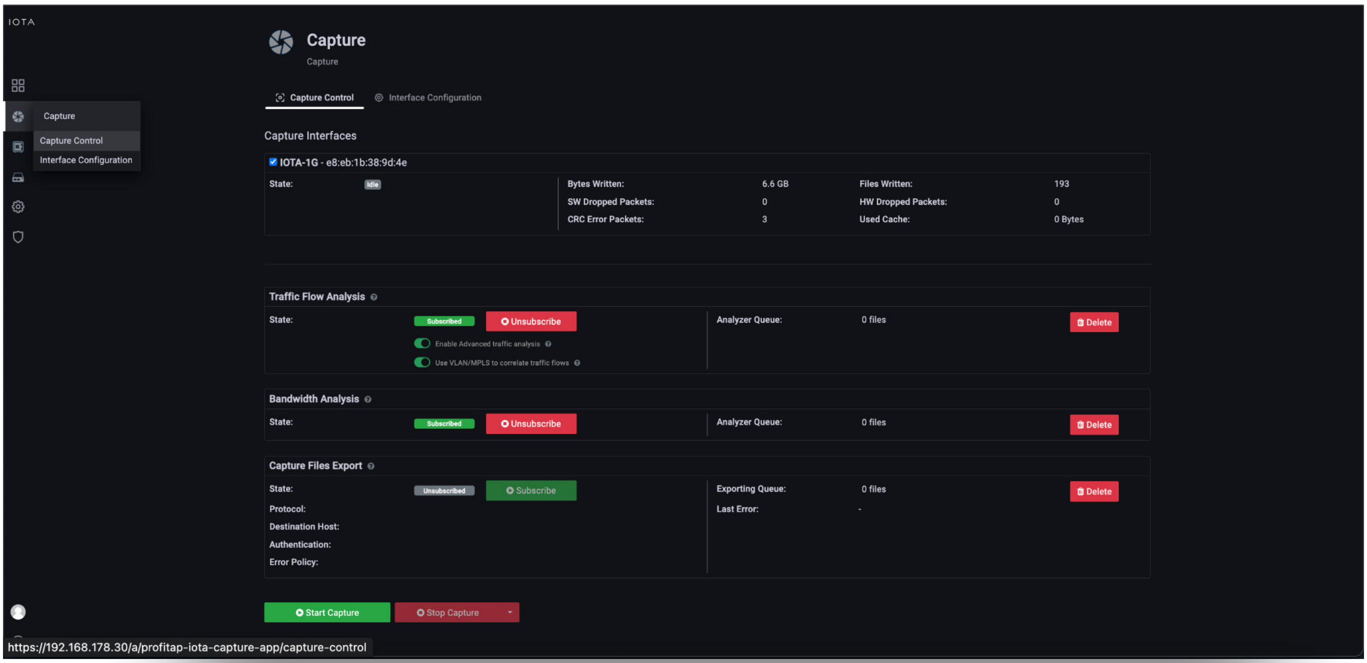
Port B 1Gbps_FDX

☑ 1000TX-FD ☑ 100TX-FD
☑ 100TX-HD ☑ 10TX-FD
☑ 10TX-HD ☑ Autonegotiation
☑ Symmetric Pause ☑ Asymmetric Pause
☐ Master ☐ Force Master/Slave

https://192.168.178.30/a/profitap-iota-capture-app/interface-config

Figure 1: Configuration of the physical interfaces. In this case, 10/100/1000 Mbit/s Auto-Negotiation in SPAN mode.

After we have prepared the physical interface, we connect the corresponding cables and start the capture process on the **Capture Control** page by clicking the **Start Capture** button.



Capture Interfaces

☑ IOTA-1G - e8:eb:1b:38:9d:4e

State:	Idle	Bytes Written:	6.6 GB	Files Written:	193
		SW Dropped Packets:	0	HW Dropped Packets:	0
		CRC Error Packets:	3	Used Cache:	0 Bytes

Traffic Flow Analysis

State: Subscribed — Unsubscribe — Analyzer Queue: 0 files — Delete

Enable Advanced traffic analysis (on)

Use VLAN/MPLS to correlate traffic flows (on)

Bandwidth Analysis

State: Subscribed — Unsubscribe — Analyzer Queue: 0 files — Delete

Capture Files Export

State: Unsubscribed — Subscribe — Exporting Queue: 0 files — Delete

Protocol:

Destination Host:

Authentication:

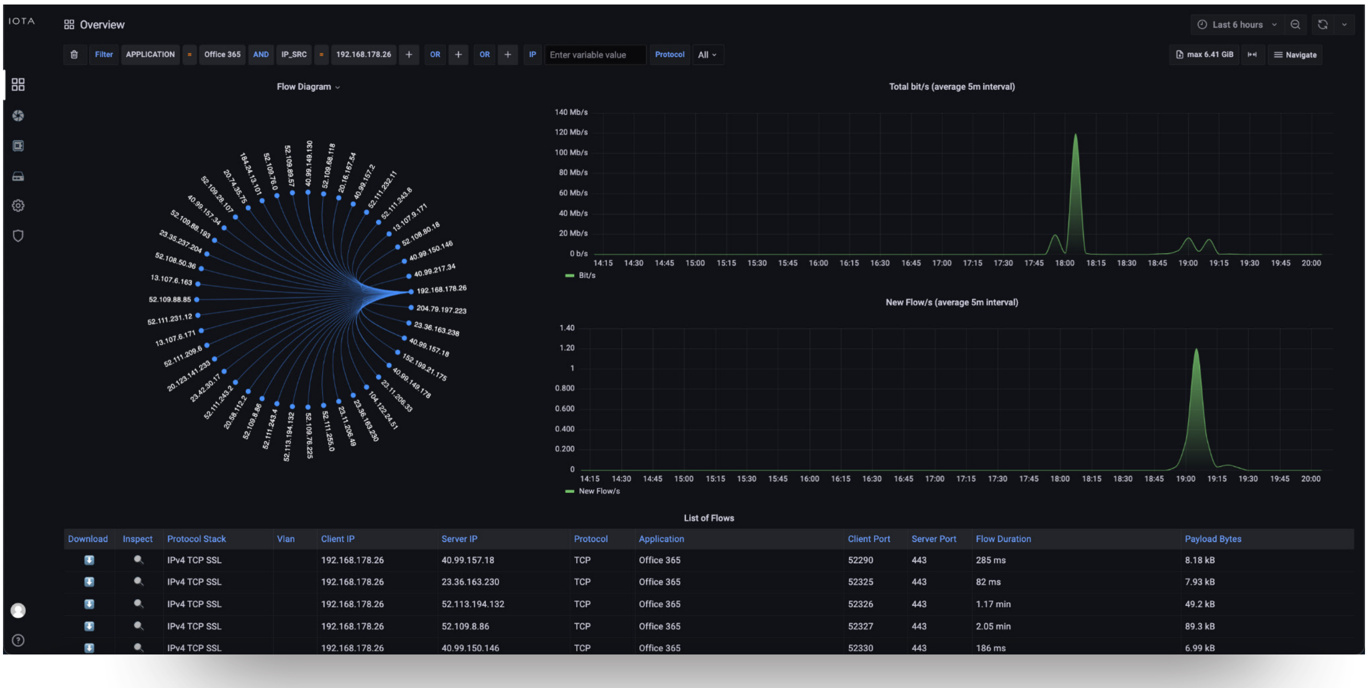
Error Policy:

Last Error: -

https://192.168.178.30/a/profitap-iota-capture-app/capture-control

Figure 2: Starting the capture via the "Start Capture" button on the "Capture Control" page

First, we set a filter on the **Overview** dashboard for the Office 365 application and the source IP address of the affected client. This allows us to quickly narrow down the affected communication relationship



List of Flows

Download	Inspect	Protocol Stack	Vlan	Client IP	Server IP	Protocol	Application	Client Port	Server Port	Flow Duration	Payload Bytes
⬇	🔍	IPv4 TCP SSL		192.168.178.26	40.99.157.18	TCP	Office 365	52290	443	285 ms	8.18 kB
⬇	🔍	IPv4 TCP SSL		192.168.178.26	23.36.163.230	TCP	Office 365	52325	443	82 ms	7.93 kB
⬇	🔍	IPv4 TCP SSL		192.168.178.26	52.113.194.132	TCP	Office 365	52326	443	1.17 min	49.2 kB
⬇	🔍	IPv4 TCP SSL		192.168.178.26	52.109.8.86	TCP	Office 365	52327	443	2.05 min	89.3 kB
⬇	🔍	IPv4 TCP SSL		192.168.178.26	40.99.150.146	TCP	Office 365	52330	443	186 ms	6.99 kB

Figure 3: Filter on Office 365 and source IP address of the client; in this case, 192.168.178.26.

Since Office 365 establishes TCP communication on port 443 (HTTPS) to the respective target server, we focus on this communication pattern. To do this, we switch to the **TCP Analysis** dashboard via the **Navigate** menu in the upper right corner of the screen.

In the **TCP Analysis** dashboard, we immediately recognize the strong spike of the initial round trip time to the server '52.111.232.11' and the server hostname 'messaging.engagement.office.com' using the descending iRTT sorting.

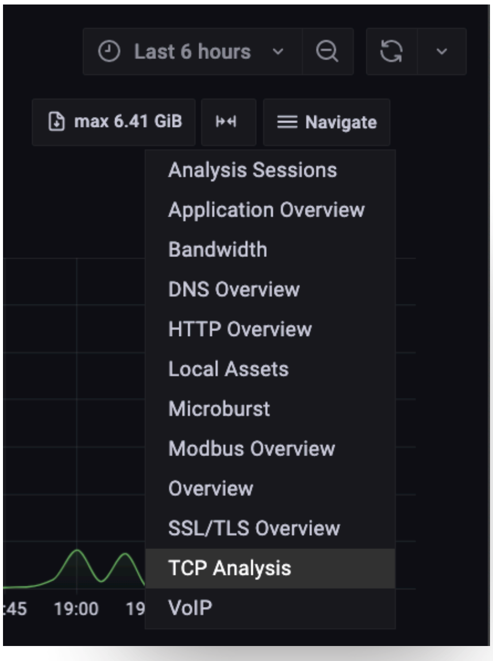
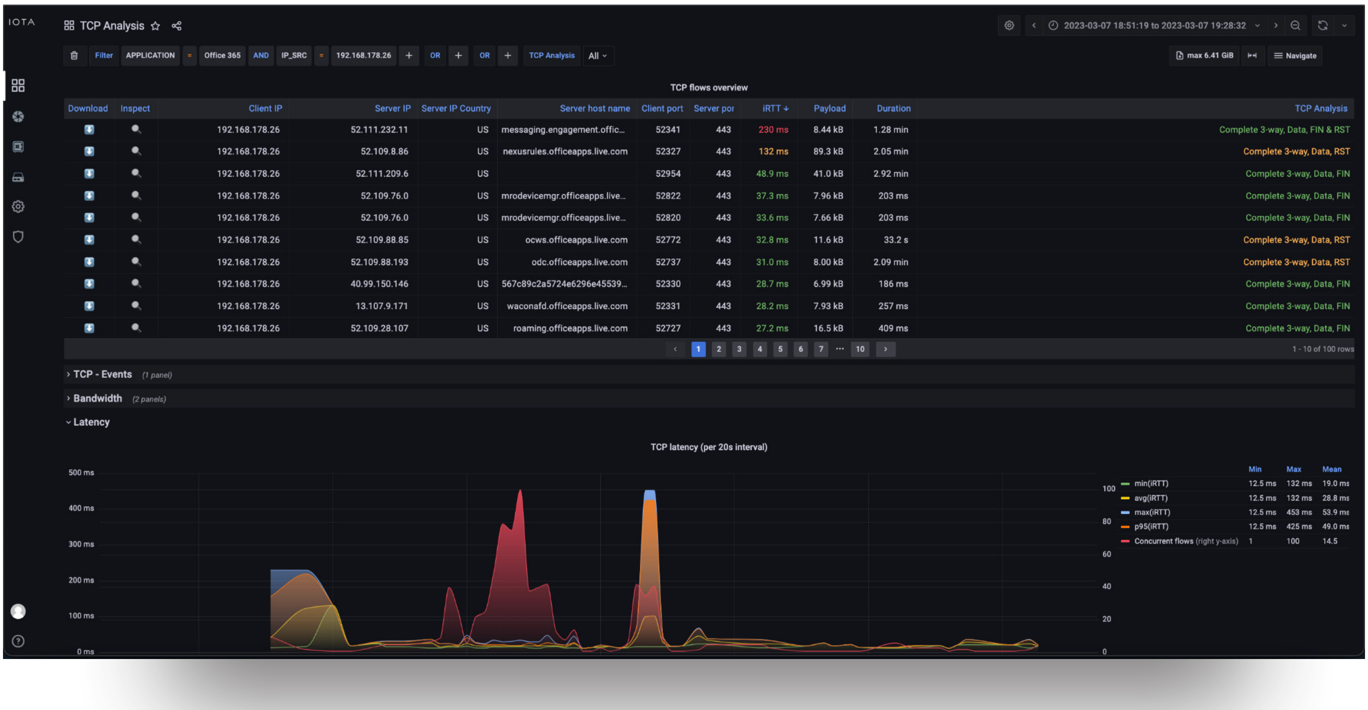


Figure 4: Switch to TCP Analysis.



TCP flows overview

Download	Inspect	Client IP	Server IP	Server IP Country	Server host name	Client port	Server por	iRTT ↓	Payload	Duration	TCP Analysis
⬇	🔍	192.168.178.26	52.111.232.11	US	messaging.engagement.offic...	52341	443	230 ms	8.44 kB	1.28 min	Complete 3-way, Data, FIN & RST
⬇	🔍	192.168.178.26	52.109.8.86	US	nexusrules.officeapps.live.com	52327	443	132 ms	89.3 kB	2.05 min	Complete 3-way, Data, RST
⬇	🔍	192.168.178.26	52.111.209.6	US		52954	443	48.9 ms	41.0 kB	2.92 min	Complete 3-way, Data, FIN
⬇	🔍	192.168.178.26	52.109.76.0	US	mrodevicemgr.officeapps.live...	52822	443	37.3 ms	7.96 kB	203 ms	Complete 3-way, Data, FIN
⬇	🔍	192.168.178.26	52.109.76.0	US	mrodevicemgr.officeapps.live...	52820	443	33.6 ms	7.66 kB	203 ms	Complete 3-way, Data, FIN
⬇	🔍	192.168.178.26	52.109.88.85	US	ocws.officeapps.live.com	52772	443	32.8 ms	11.6 kB	33.2 s	Complete 3-way, Data, RST
⬇	🔍	192.168.178.26	52.109.88.193	US	odc.officeapps.live.com	52737	443	31.0 ms	8.00 kB	2.09 min	Complete 3-way, Data, RST
⬇	🔍	192.168.178.26	40.99.150.146	US	567c89c2a5724e6296e45539...	52330	443	28.7 ms	6.99 kB	186 ms	Complete 3-way, Data, FIN
⬇	🔍	192.168.178.26	13.107.9.171	US	waconafd.officeapps.live.com	52331	443	28.2 ms	7.93 kB	257 ms	Complete 3-way, Data, FIN
⬇	🔍	192.168.178.26	52.109.28.107	US	roaming.officeapps.live.com	52727	443	27.2 ms	16.5 kB	409 ms	Complete 3-way, Data, FIN

‹ 1 2 3 4 5 6 7 ··· 10 › 1 - 10 of 100 rows

› TCP - Events *(1 panel)*

› Bandwidth *(2 panels)*

⌄ Latency

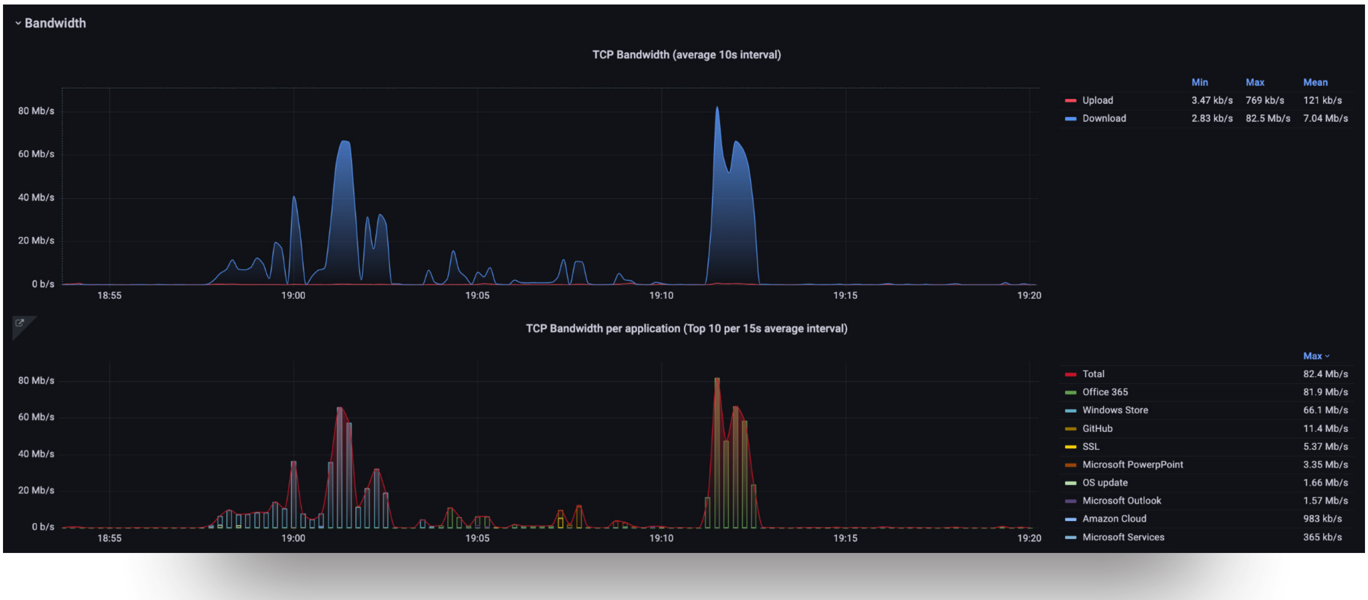
TCP latency (per 20s interval)

	Min	Max	Mean
min(iRTT)	12.5 ms	132 ms	19.0 ms
avg(iRTT)	12.5 ms	132 ms	28.8 ms
max(iRTT)	12.5 ms	453 ms	53.9 ms
p95(iRTT)	12.5 ms	425 ms	49.0 ms
Concurrent flows (right y-axis)	1	100	14.5

Figure 5: "TCP Analysis" dashboard.

To identify possible bandwidth bottlenecks, bandwidth graphs are available in the **TCP Analysis** dashboard. These show the total TCP bandwidth used for the data recorded in the interval and a display and listing for each application.

Low bandwidth usage can be caused by missing window scaling flags in the TCP header, for example, or simply by other transmissions that are transported in parallel over the same connection and share the available bandwidth.



⌄ Bandwidth

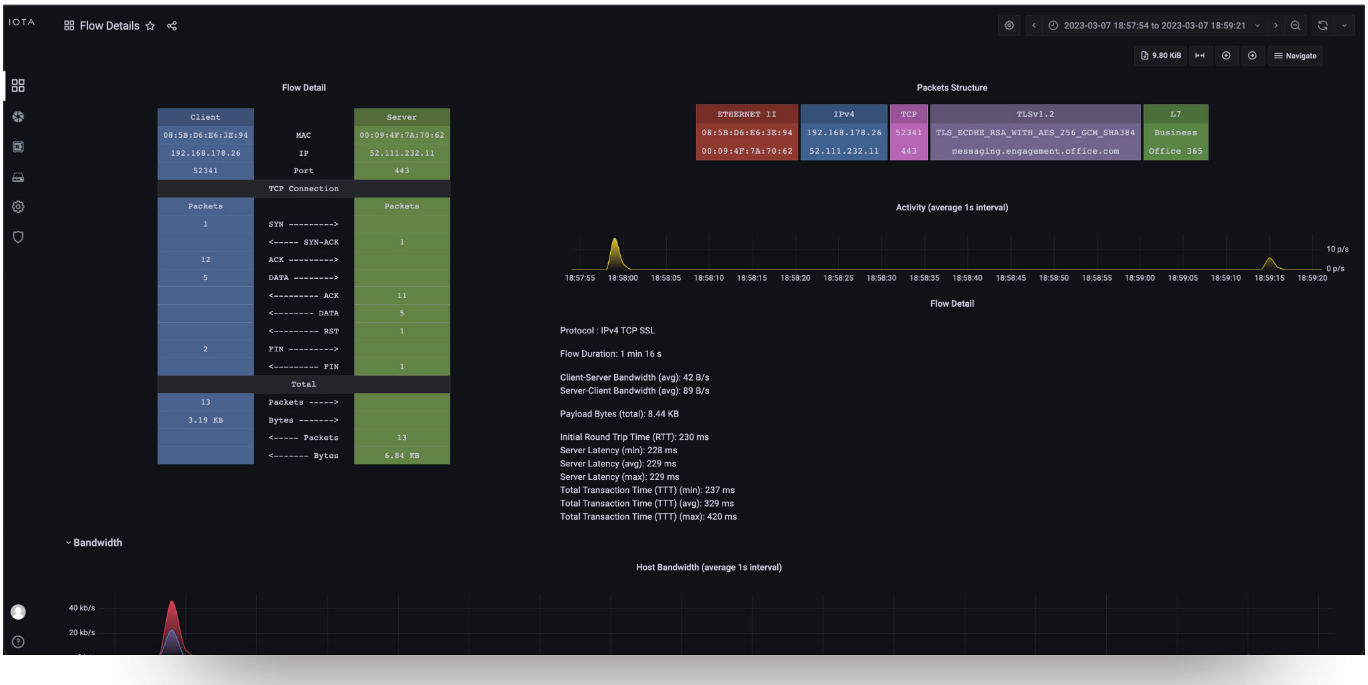
TCP Bandwidth (average 10s interval)

	Min	Max	Mean
Upload	3.47 kb/s	769 kb/s	121 kb/s
Download	2.83 kb/s	82.5 Mb/s	7.04 Mb/s

TCP Bandwidth per application (Top 10 per 15s average interval)

	Max ⌄
Total	82.4 Mb/s
Office 365	81.9 Mb/s
Windows Store	66.1 Mb/s
GitHub	11.4 Mb/s
SSL	5.37 Mb/s
Microsoft PowerPoint	3.35 Mb/s
OS update	1.66 Mb/s
Microsoft Outlook	1.57 Mb/s
Amazon Cloud	983 kb/s
Microsoft Services	365 kb/s

Figure 6: Bandwidth graphs of the "TCP Analysis" dashboard. The upper graph displays the total bandwidth and below the bandwidth per application.



Flow Detail

Client		Server
08:5B:D6:E6:3E:94	MAC	00:09:4F:7A:70:62
192.168.178.26	IP	52.111.232.11
52341	Port	443
	TCP Connection	
Packets		Packets
1	SYN --------->	
	<----- SYN-ACK	1
12	ACK --------->	
5	DATA -------->	
	<--------- ACK	11
	<-------- DATA	5
	<--------- RST	1
2	FIN --------->	
	<--------- FIN	1
	Total	
13	Packets ----->	
3.19 KB	Bytes ------->	
	<----- Packets	13
	<------- Bytes	6.84 KB

Packets Structure

ETHERNET II	IPv4	TCP	TLSv1.2	L7
08:5B:D6:E6:3E:94	192.168.178.26	52341	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Business
00:09:4F:7A:70:62	52.111.232.11	443	messaging.engagement.office.com	Office 365

Flow Detail

Protocol : IPv4 TCP SSL

Flow Duration: 1 min 16 s

Client-Server Bandwidth (avg): 42 B/s
Server-Client Bandwidth (avg): 89 B/s

Payload Bytes (total): 8.44 KB

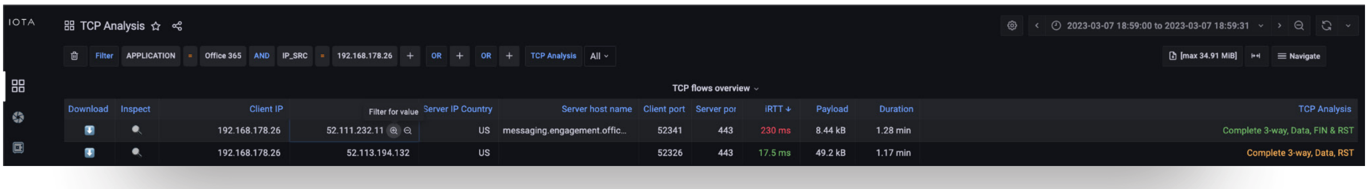
Initial Round Trip Time (RTT): 230 ms
Server Latency (min): 228 ms
Server Latency (avg): 229 ms
Server Latency (max): 229 ms
Total Transaction Time (TTT) (min): 237 ms
Total Transaction Time (TTT) (avg): 329 ms
Total Transaction Time (TTT) (max): 420 ms

Figure 7: TCP Flow Detail dashboard.

Since, according to the descending list of iRTT in the **TCP Analysis** dashboard, only this one server has such a high initial round trip time in the specified time window, and other target servers in the same autonomous system from Microsoft are considerably lower, it can be assumed that there is a performance problem bottleneck in the network connection to the server in the Microsoft network or a bottleneck on the server itself. However, since the server latency is roughly in the same range as the iRTT according to the information in the **Flow Detail** dashboard, it can be assumed that there is a high latency in the connection of this server at Microsoft. This is because when there is a performance bottleneck on the server, the iRTT is usually in the normal range, but the server latency is very high. The behavior shown resulted in a sluggish application.

However, sluggish applications can also have TCP retransmissions due to packet loss or sluggish servers or clients. To evaluate these, we return to the **TCP Analysis** dashboard.

In this dashboard, we now filter based on the server's destination IP address by hovering over the destination IP address and clicking the + icon to activate the filter.



Filter APPLICATION = Office 365 AND IP_SRC = 192.168.178.26 + OR + OR + TCP Analysis All

TCP flows overview

Download	Inspect	Client IP	Filter for value	Server IP Country	Server host name	Client port	Server por	iRTT ↓	Payload	Duration	TCP Analysis
		192.168.178.26	52.111.232.11	US	messaging.engagement.offic...	52341	443	230 ms	8.44 kB	1.28 min	Complete 3-way, Data, FIN & RST
		192.168.178.26	52.113.194.132	US		52326	443	17.5 ms	49.2 kB	1.17 min	Complete 3-way, Data, RST

Figure 8: Creating a filter on the server IP address 52.111.232.11 by clicking the + symbol next to the IP address.

After setting the filter, we look at the **TCP Retransmission** graph at the bottom of the dashboard. Here, we can see that there were client-side retransmissions in the same time period. This means that the client either did not receive the requested data or acknowledgments (ACKs) or received them late and therefore started a retransmission. An analysis at other points of the communication path would have to provide precise information about where the error originated.

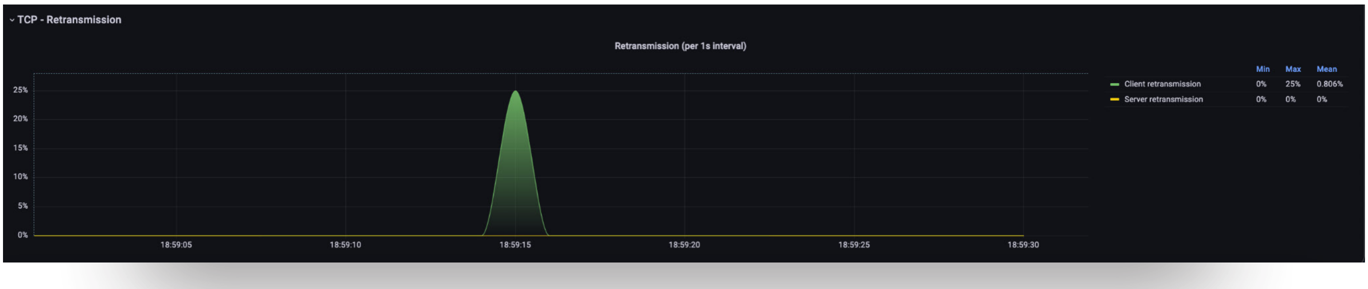
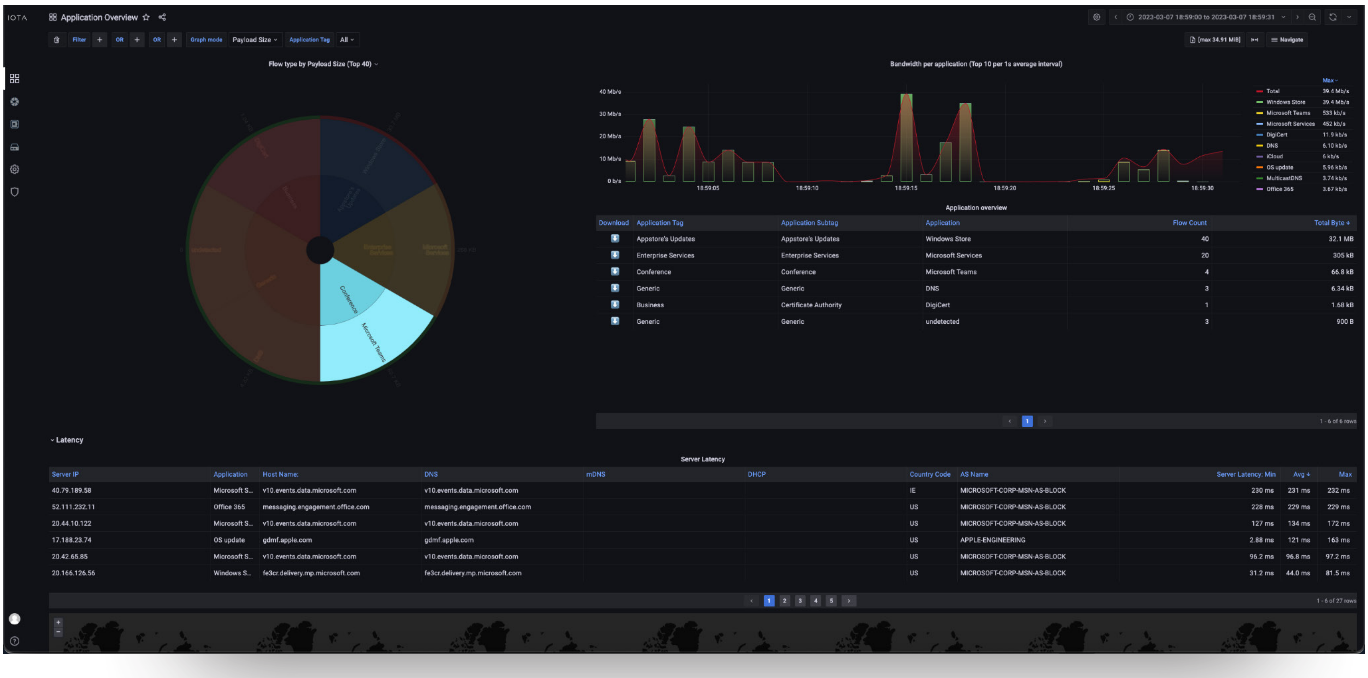


Figure 9: TCP retransmission graph of the filtered connection.

The Application Overview dashboard can also provide a further indication of sluggish applications. In this dashboard, different applications, such as Microsoft Teams in the example shown, can be filtered based on a pie chart and displayed with bandwidth and latency in different graphs and tables.



Application overview

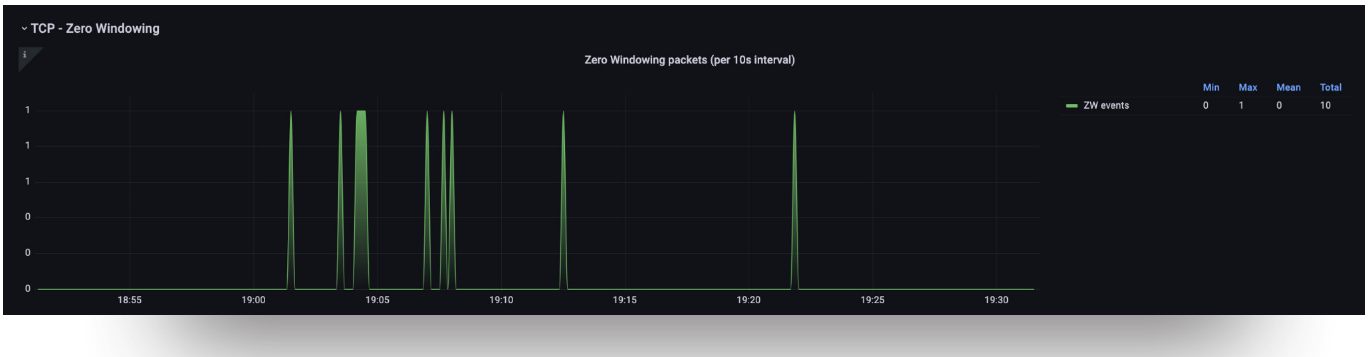
Download	Application Tag	Application Subtag	Application	Flow Count	Total Byte ↓
⬇	Appstore's Updates	Appstore's Updates	Windows Store	40	32.1 MB
⬇	Enterprise Services	Enterprise Services	Microsoft Services	20	305 kB
⬇	Conference	Conference	Microsoft Teams	4	66.8 kB
⬇	Generic	Generic	DNS	3	6.34 kB
⬇	Business	Certificate Authority	DigiCert	1	1.68 kB
⬇	Generic	Generic	undetected	3	900 B

Server Latency

Server IP	Application	Host Name:	DNS	mDNS	DHCP	Country Code	AS Name	Server Latency: Min	Avg ↓	Max
40.79.189.58	Microsoft S...	v10.events.data.microsoft.com	v10.events.data.microsoft.com			IE	MICROSOFT-CORP-MSN-AS-BLOCK	230 ms	231 ms	232 ms
52.111.232.11	Office 365	messaging.engagement.office.com	messaging.engagement.office.com			US	MICROSOFT-CORP-MSN-AS-BLOCK	228 ms	229 ms	229 ms
20.44.10.122	Microsoft S...	v10.events.data.microsoft.com	v10.events.data.microsoft.com			US	MICROSOFT-CORP-MSN-AS-BLOCK	127 ms	134 ms	172 ms
17.188.23.74	OS update	gdmf.apple.com	gdmf.apple.com			US	APPLE-ENGINEERING	2.88 ms	121 ms	163 ms
20.42.65.85	Microsoft S...	v10.events.data.microsoft.com	v10.events.data.microsoft.com			US	MICROSOFT-CORP-MSN-AS-BLOCK	96.2 ms	96.8 ms	97.2 ms
20.166.126.56	Windows S...	fe3cr.delivery.mp.microsoft.com	fe3cr.delivery.mp.microsoft.com			US	MICROSOFT-CORP-MSN-AS-BLOCK	31.2 ms	44.0 ms	81.5 ms

Figure 10: Application Overview dashboard with bandwidth graphs, filtering option based on a pie chart, and a tabular latency overview.

Another error pattern was that the application froze intermittently. A possible cause for a freezing application can be TCP Zero Windows. This means that the packet was delivered on the network side but could not be retrieved by the application from the TCP/IP stack of the operating system. Consequently, the TCP/IP stack signals this to the remote peer. The cause of such behavior is a performance bottleneck at the sender of the Zero Windows. We can then drill down to narrow the scope of the Zero Window message and then filter the flows. In the Zero Windows plot below, we can see at what times these occurred.

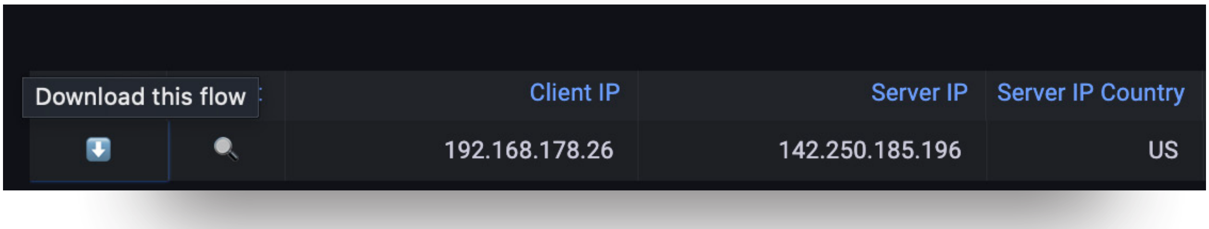


	Min	Max	Mean	Total
🟩 ZW events	0	1	0	10

Figure 11: Representation of TCP Zero Window messages.

To detect who sent the Zero Window message, there is then the possibility of a PCAPNG download via the arrow button on the left in the image below.

Using the display filter 'tcp.analysis.zero_window' in Wireshark, it is very easy to determine the sender of the Zero Window.



		Client IP	Server IP	Server IP Country
⬇	🔍	192.168.178.26	142.250.185.196	US

Figure 12: Download a PCAPNG file for analysis in Wireshark

About the IOTA Solution

The IOTA provides an integrated recording and analysis platform for networks. Based on intuitive dashboards, it is possible to apply performant and diverse filters to determine the root cause of the faulty communication relationship and consequently shorten the mean-time-to-repair. The application intelligence also helps to pre-filter data flows according to the application used.

IOTA LINEUP

IOTA 1G

Key capture point / Remote office

2 x RJ45
1 TB SSD

IOTA 1G+

Key capture point / Remote office

2 x RJ45
1 TB or 2 TB Removable SSD
GPS/PPS timing ports

IOTA 10G

Large Branch / WAN edge

2 x SFP / SFP+
1 TB SSD

IOTA 10G+

Large Branch / WAN edge

2 x SFP / SFP+
1 TB or 2 TB Removable SSD
GPS/PPS timing ports

FIND OUT MORE ON WWW.PROFITAP.COM/IOTA

Profitap HQ B.V.
High Tech Campus 84
5656 AG Eindhoven
The Netherlands

sales@profitap.com
www.profitap.com

Profitap
@Profitap
Profitap-international