

PROFITAP

PRODUCT PORTFOLIO

PROFITAP SOLUTIONS BRING CLARITY
INTO YOUR NETWORKS



TRAFFIC
ACCESS



MANAGING AND
OPTIMIZING
DATA FLOW



TRAFFIC
CAPTURE &
ANALYSIS

PROFITAP: THE COMPANY

High Tech Campus — Eindhoven

Profitap develops and manufactures a complete range of innovative Network TAPs, Network Packet Brokers and Field Service Troubleshooters for the security, forensics, deep packet capture and network performance monitoring sectors. All of Profitap's network monitoring solutions are highly performant and user-friendly, providing complete visibility and access to your network, 24/7.

Premium Quality Products

Profitap provides hardware and software solutions for network analysis and traffic acquisition to organizations and professionals globally. With our solutions being front-runners in the IT industry, we have fused high performance with security to create exclusive, industry leading monitoring solutions.

Profitap devices use hardware embedded field-programmable gate array (FPGA) technologies, resulting in extremely low latency. With non-intrusive and fail-safe designs, Profitap network analysis and traffic acquisition solutions send all required data to your security appliances to easily prevent and analyze cyberthreats.

All devices are subject to a zero failure production regime and following this are stress tested, and in the case of fiber TAPs microscopically inspected to ensure that the optics are dust free.

An Innovative Brand

With our experience, we manufacture and deliver exceptionally designed, innovative monitoring solutions. We have developed our products to set new standards in an industry where the definition of excellence is constantly being challenged.

Constantly Improving Our Technology

Profitap is self-funded and has an enviable successful financial track record with investment in Research and Development (R&D) being significantly above the market average. This results in the release of innovative devices that are unique in the market.

Global Coverage

With more than 1.000 clients from 55 countries, Profitap has become an integral solution for major businesses, many of which are Fortune Global 500 companies.

Easy To Work With

We offer access to our technical support desk as a single point of contact for technical queries and all the product support you need to lead, close and succeed.

Experienced Partner Community

Our Partners are fully trained and certified in Profitap's solutions. They are selected for their technical expertise and high standards of customer service. This ensures that working with Profitap solutions is simple, so you can concentrate on running your business.

CONTENTS

01

TRAFFIC ACCESS

Copper TAPs
Fiber TAPs
Aggregation TAPs
Bypass TAPs
Secure Data Access Solutions
Virtual TAP

02

MANAGING AND OPTIMIZING DATA FLOW

XX-Series Network Traffic Aggregators
X2-Series Network Packet Brokers
X3-Series Network Packet Brokers
NPB Management
Supervisor

03

TRAFFIC CAPTURE AND ANALYSIS

ProfShark
IOTA

TRAFFIC ACCESS

Access network traffic at key capture points in physical and virtual networks

A reliable source of packet data for monitoring solutions

Network analysis starts with getting actionable data in a reliable and secure way. While there are many ways to capture packets on a live network, there are often serious downsides, such as packet loss, out of order packets, or the use of devices that can be used in man-in-the-middle attacks. All of this directly impacts the quality of analysis and the security of the network itself. A best practice here is to deploy network TAPs (test access points) as the key method for accessing network traffic. TAPs are hardware devices deployed at key locations between two points in network infrastructure, such as routers, switches, or firewalls, where data access is needed for monitoring or troubleshooting purposes. In a virtual environment, a virtual TAP, or vTAP, is installed on the virtualized server, providing full access and visibility into the east-west traffic flows.

Purpose built, network TAPs are more reliable than switch port analyzer (SPAN) ports, particularly at high data rates. Network TAPs offer significant advantages over the use of SPAN ports to monitor the network, such as providing access to packets of all sizes and types at wire speed, delivering an exact copy of all traffic to the monitoring ports, and isolating monitoring devices from the network to mitigate the risk of data breaches.

Network TAPs enable you to:

- Achieve complete access and visibility across your physical and virtual networks.
- Obtain fail-safe, permanent in-line network access to live traffic in high-speed networks.
- Protect the network link availability for in-line security tools.
- Eliminate the risk of single points of failure in accessing the network traffic.
- Deliver lossless traffic aggregation from multiple in-line links or out-of-band connections.

COPPER TAPS

COMPLETE ACCESS AND VISIBILITY INTO YOUR COPPER NETWORKS

Profitap Copper TAPs provide complete visibility into your network by creating an exact copy of full-duplex 10M/100M/1G/10G traffic at wire speed with no impact on the network link, allowing monitoring devices to be connected and disconnected as desired.

To maintain the network connection and prevent any interruption in traffic flow, all Profitap Active Copper TAPs feature a No Break fail-safe functionality, a quick switching mechanism that activates in case of power loss. Profitap Copper TAPs are equipped with high-speed relays that ensure a very short network recovery time. This means that the traffic received from the network will pass through the TAPs even when the power is disrupted.

No Break

PROFITAP® Copper TAPs feature dramatically reduced failover time, consequently reducing the chances of Spanning Tree reconvergence.

Link Failure Propagation

PROFITAP® Copper TAPs transmit link failure errors between ports, allowing the network to activate a redundant path, while the TAP stays available for auto-negotiation. LFP ensures less downtime, and is essential for high availability networks.

Full Visibility

PROFITAP® Copper TAPs monitor all 7 OSI layers, packets of all sizes and types, and low-level errors, making sure not a single packet is lost.

Network Security

PROFITAP® Copper TAPs are non-intrusive, have no IP address, and isolate monitoring devices from the network to ensure complete stealth and security at all times.

Fail-Safe

PROFITAP® Copper TAPs introduce no point of failure to the network and feature redundant powering. In case of complete power failure, our TAPs guarantee that the link remains operational by instantly switching to a fully passive mode.

Eco-friendly

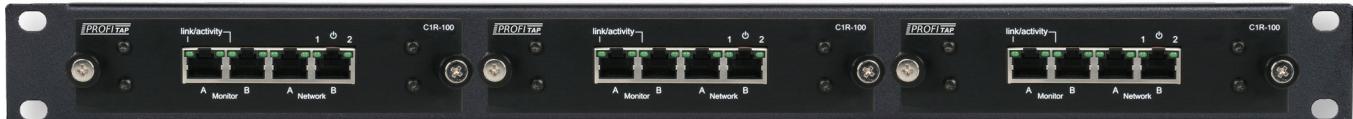
At PROFITAP®, we believe it is the collective responsibility of the IT industry to keep our environment as clean as possible by using green products and contribute to reducing the global carbon footprint. We commit ourselves to producing premium quality and environment-friendly products. With the lowest power consumption on the market.

Compliance

All Copper TAPs are fully 802.3af, VoIP, and PoE compliant.

100M COPPER TAPS

Model	Speed	NET	TAP	Footprint
C1R-100	10/100 Mbps	1	1	Up to 3 in 1U
C20-100	10/100 Mbps	20	20	1U
C1D-100	10/100 Mbps	1	1	Portable



C1R-100 (3 products in 1U)



C20-100



C1D-100

1G COPPER TAPS

Model	Speed	NET	TAP	Footprint
C1R-1G	10/100/1000 Mbps	1	1	Up to 3 in 1U
C1R-1G-48V	10/100/1000 Mbps	1	1	Up to 3 in 1U
C1R-1G-BAT	10/100/1000 Mbps	1	1	Up to 3 in 1U
C8-1G	10/100/1000 Mbps	8	8	1U



C1R-1G

C1R-1G-48V

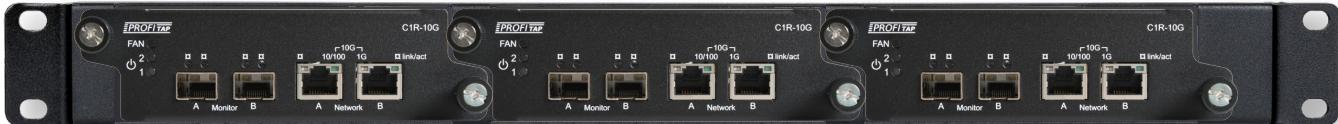
C1R-1G-BAT



C8-1G

10G COPPER TAPS

Model	Speed	NET	TAP	Footprint
C1R-10G	10M/100M/1G/10G	1	1	Up to 3 in 1U



C1R-10G (3 products in 1U)

DUAL OUTPUT GIGABIT COPPER TAPS

Model	Speed	NET	TAP	Footprint
C1-1G-RG2	10/100/1000 Mbps	1	2	Up to 3 in 1U



C1-1G-RG2 (3 products in 1U)

GIGABIT COPPER PORT REPLICATOR

Model	Speed	NET	TAP	Footprint
CS1G-C4G	10/100/1000 Mbps	1	4	Up to 3 in 1U



CS1G-C4G (3 products in 1U)

Visit our website and request a quote
for more information.

www.profitap.com/copper-taps ►

FIBER TAPS

RELIABLE, SECURE TRAFFIC ACCESS FOR YOUR FIBER NETWORKS

Profitap Fiber TAPs provide fail-safe in-line monitoring of 1-400 Gbps fiber networks, monitor all 7 OSI layers, packets of all sizes and types, and low-level errors. By splitting light flowing on the network link, Profitap Fiber TAPs deliver an exact copy of the data for real-time monitoring and analysis without disrupting the network.

As fully passive devices, Profitap Fiber TAPs require no power, and therefore introduce no point of failure when deployed in a network. Profitap Fiber TAPs provide access to data flowing across a network, without interrupting the data flow. Profitap Fiber TAPs are extensively tested before and after assembly by our team of experts and are available in various split ratios and configurations to meet your specific requirements.

Full Visibility

PROFITAP® Fiber TAPs deliver an exact copy of the traffic by splitting the optical signal flowing on the network link.

10 Year Warranty

PROFITAP® Passive Fiber TAPs are covered by a 10-year warranty, proof of the confidence we place in our products.

Network Security

PROFITAP® Fiber TAPs are non-intrusive, have no IP address, and isolate monitoring devices from the network to ensure complete stealth and security at all times.

Extensive Testing Procedure

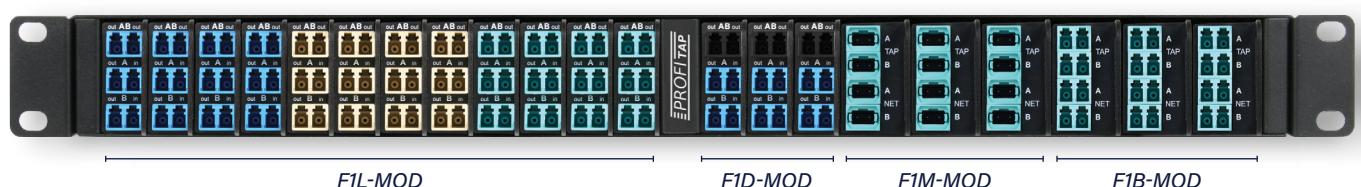
Every single one of our fiber components is extensively tested before and after assembly by our team of experts.

Fail-Safe

PROFITAP® Fiber TAPs introduce no point of failure to the network because they are fully passive, so they require no additional powering. This way a permanent link is guaranteed.

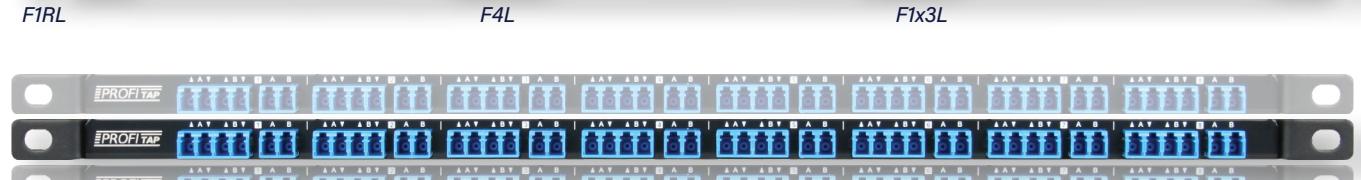
MODULAR TAPS

Model	Speed	Fiber Type	Wavelength	Split Ratio	Passive	Conn.	NET	TAP	Footprint	Power
F1L-MOD	1 Gbps	MM 62.5 µm	850/1300 nm	50/50 60/40 70/30	Yes	LC	1	1	Up to 24 in 1U	—
	1-100 Gbps	MM 50 µm OM4	850/1300 nm	50/50 60/40 70/30						
	1-100 Gbps	MM 50 µm OM5	850/1300 nm	50/50 60/40 70/30						
	1-400 Gbps	SM 9 µm OS2	1310/1550 nm	50/50 60/40 70/30						
F1B-MOD	40/100 Gbps	MM 50 µm OM4	850–950 nm	50/50	Yes	LC	1	1	Up to 16 in 1U	—
	40/100 Gbps	MM 50 µm OM5	850–950 nm	50/50 60/40						
F1M-MOD	40 Gbps	MM 40GBASE-SR4	850/1300 nm	50/50	Yes	MTP/MPO	1	1	Up to 16 in 1U	—
	100 Gbps	MM 100GBASE-SR4	850/1300 nm	50/50						
	100 Gbps	MM 100GBASE-SR10	850/1300 nm	50/50						
	40 Gbps	SM 40GBASE-PLR4	1310/1550 nm	50/50 70/30						
	100 Gbps	SM 100GBASE-PSM4	1310/1550 nm	50/50 70/30						
F1D-MOD	1-400 Gbps	SM 9/125 µm	1310/1550 nm	50/50 60/40	Yes	LC	1	1	Up to 16 in 1U Up to 6 in 1U	—
	1-25 Gbps	MM 50/125 µm	850 nm	50/50 60/40						



LC FIBER TAPS

Model	Speed	Fiber Type	Wavelength	Split Ratio	Passive	Conn.	NET	TAP	Footprint	Power
F1RL	1 Gbps	MM 62.5 µm	850/1300 nm	50/50 60/40 70/30 80/20	Yes	LC	1	1	Up to 3 in 1U	—
	1-25 Gbps	MM 50 µm OM4	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	MM 50 µm OM5	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	SM 9 µm	1310/1550 nm	50/50 60/40 70/30 80/20						
F1PL	1 Gbps	MM 62.5 µm	850/1300 nm	50/50 60/40 70/30 80/20	Yes	LC	1	1	Portable	—
	1-25 Gbps	MM 50 µm OM4	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	MM 50 µm OM5	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	SM 9 µm	1310/1550 nm	50/50 60/40 70/30 80/20						
F4L	1 Gbps	MM 62.5 µm	850/1300 nm	50/50 60/40 70/30 80/20	Yes	LC	4	4	Up to 3 in 1U	—
	1-25 Gbps	MM 50 µm OM4	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	MM 50 µm OM5	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	SM 9 µm	1310/1550 nm	50/50 60/40 70/30 80/20						
F8L	1 Gbps	MM 62.5 µm	850/1300 nm	50/50 60/40 70/30 80/20	Yes	LC	8	8	Up to 3 in 1U	—
	1-25 Gbps	MM 50 µm OM4	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	MM 50 µm OM5	850/1300 nm	50/50 60/40 70/30 80/20						
	1-100 Gbps	SM 9 µm	1310/1550 nm	50/50 60/40 70/30 80/20						
F1x3L	1-100 Gbps	MM 50/125 µm	850/1300 nm	50/25/25 40/30/30	Yes	LC	1	2	Up to 3 in 1U	—
	1-100 Gbps	SM 9/125 µm	1310/1550 nm	50/25/25 40/30/30						



REGENERATION TAPS

Model	Speed	Fiber Type	Wavelength	Split Ratio	Passive	Conn.	NET	TAP	Footprint	Power
F1L-AT	1-10 Gbps	MM 50/125 µm SR	850 nm	—	Yes	LC	1	1	Up to 3 in 1U	12 VDC
	1-10 Gbps	SM 9/125 µm LR	1310 nm							
	1-10 Gbps	SM 9/125 µm ER	1310 nm							
	1-10 Gbps	SM 9/125 µm ZR	1310 nm							
	1-10 Gbps	SM 9/125 µm LR (-16dBm)	1310 nm							
F1L-RG2	1/10 Gbps	MM 50 µm	850 nm	50/50 60/40	Yes	LC	1	2	Up to 3 in 1U	12 VDC
	1/10 Gbps	SM 9 µm	1310 nm	50/50 60/40						
F1L-RG4	1/10 Gbps	MM 50 µm	850 nm	50/50 60/40	Yes	LC	1	4	Up to 3 in 1U	12 VDC
	1/10 Gbps	SM 9 µm	1310 nm	50/50 60/40						



F1L-AT

F1L-RG2

F1L-RG4

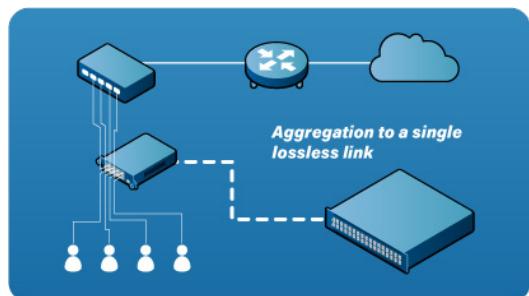
Visit our website and request a quote
for more information.

www.profitap.com/fiber-taps ▶

AGGREGATION TAPS

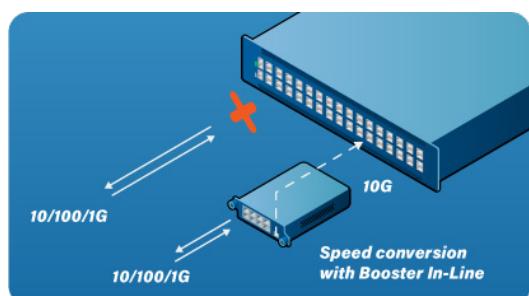
Aggregation TAPs designed for lossless traffic aggregation from multiple in-line links or out-of-band connections into a single output or two replicated outputs, optimizing port usage on monitoring tools.

Profitap Booster also operates as a speed converter, which allows you to connect tools that support different speeds together. For example, the Booster brings 10M, 100M, and 1G support on Network Packet Brokers and analysis tools that do not support speeds below 10G.



LOSSLESS AGGREGATION

Conventional Aggregation TAP solutions often feature output ports with the same speed as the network links. This causes oversubscription on the output port of the TAP, causing valuable packets to be lost. By aggregating network traffic to a 10 Gbps output, no packet loss occurs. Whether traffic is forwarded to a Network Packet Broker or an IOTA, the Profitap Booster delivers lossless aggregation, while also reducing network complexity.



SPEED CONVERSION

Many high throughput devices like network packet brokers feature ports designed for 40/100 Gbps operation. With breakout cables, individual connections at 10 Gbps can be established, but lower speeds are often not a possibility. This means that lower speed links, such as 100M, cannot be forwarded directly to the toolset.

The Profitap Booster converts these links into a 10 Gbps output, bringing additional speeds to new and existing tools in a cost-effective way.

BOOSTERS

Model	Network Ports	Monitor Port	Footprint	Power
C8R-X1	8 x RJ45 10/100/1000 Mbps	1 x SFP+ 1/10 Gbps	Up to 3 in 1U	12 VDC
F8R-X1	8 x SFP 10/100/1000 Mbps	1 x SFP+ 1/10 Gbps	Up to 3 in 1U	12 VDC
C8R-X2	8 x RJ45 10/100/1000 Mbps	2 x SFP+ 1/10 Gbps	Up to 3 in 1U	12 VDC
F8R-X2	8 x SFP 10/100/1000 Mbps	2 x SFP+ 1/10 Gbps	Up to 3 in 1U	12 VDC



C8R-X1

F8R-X1

C8R-X1

Visit our website and request a quote for more information.

www.profitap.com/aggregation-taps ►

BYPASS TAPS

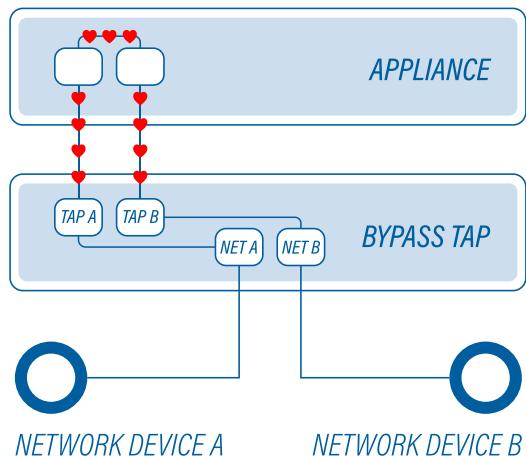
THE KEY FOR KEEPING YOUR NETWORK SAFE AND SECURE

Bypass TAPs provide fail-safe access for active in-line network security and performance tools. In the event that an active in-line tool becomes unavailable, either due to a hardware malfunction, power loss, software problem, or planned maintenance, bypass TAPs ensure the network link stays operational.

Fail-Safe Bypass & Heartbeat

Designed to support active in-line network security and performance tools, our Bypass TAPs ensure these devices don't become single points of failure in your network. By sending heartbeat packets, they can accurately track if the connected devices are operational.

In the event that an in-line device fails, either due to a hardware malfunction, power loss, or software problem, the 10G Bypass TAP's fail-safe protection keeps the critical link up.



Model	Speeds	Fiber Type	NET input(s)	TAP output(s)	Footprint	Power
F1-10G-BP-S	1/10 Gbps	SM 9 μm	1 x LC Quad	2 x SFP+	Up to 3 in 1U	12 VDC
F1-10G-BP-Z	1/10 Gbps	MM 50 μm	1 x LC Quad	2 x SFP+	Up to 3 in 1U	12 VDC
F1-40G-BP-S	40 Gbps	SM 9 μm	2 x LC Quad	2 x QSFP+	Up to 3 in 1U	12 VDC
F1-40G-BP-Z	40 Gbps	MM 50 μm	2 x MTP/MPO	2 x QSFP+	Up to 3 in 1U	12 VDC
F4-10G-BP-S	4 x 10Gbps	SM 9 μm	2 x MTP/MPO	2 x QSFP+	Up to 3 in 1U	12 VDC
F4-10G-BP-Z	4 x 10Gbps	MM 50 μm	2 x MTP/MPO	2 x QSFP+	Up to 3 in 1U	12 VDC



F1-10G-BP

F1-40G-BP

F4-10G-BP

Visit our website and request a quote for more information.

www.profitap.com/bypass-taps ►

SECURE DATA ACCESS SOLUTIONS

UPDATED SOLUTIONS FOR A CHANGING PLAYING FIELD
Meeting the industry's security requirements

- Physical isolation from the operational network on Copper TAPs, which acts as a data diode
- Optical data diode for Fiber TAPs prevents light insertion from the monitor ports
- Secured firmware implemented on active TAPs
- Security seals prevent opening and tampering with the devices





PROFITAP vTAP

COMPLETE VISIBILITY INTO YOUR VIRTUAL NETWORKS

Profitap vTAP provides complete visibility of VM traffic (including inter-VM) for security, availability, and performance monitoring.

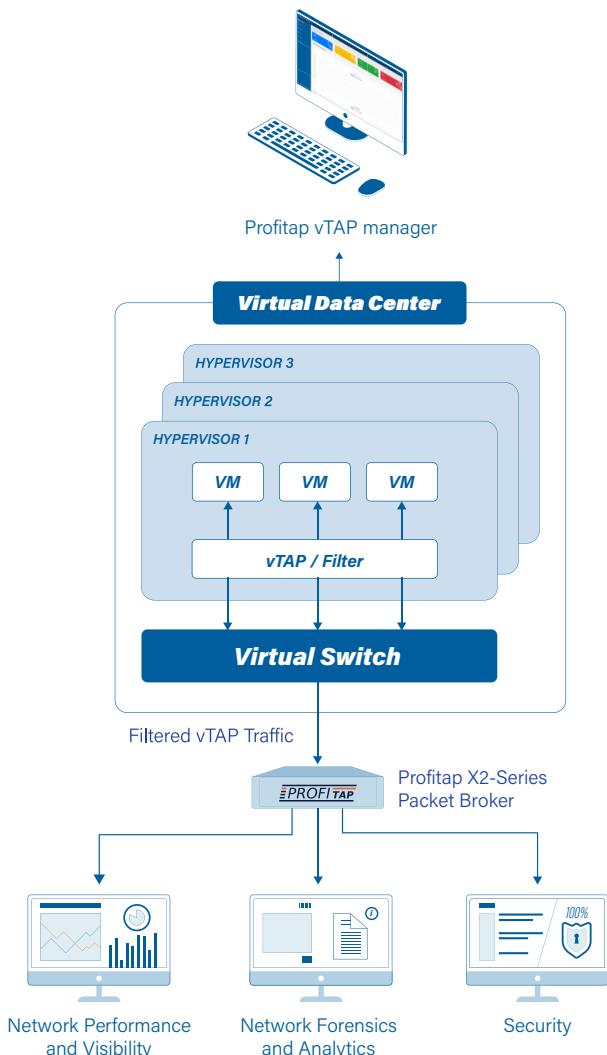
Within the span of a decade, the use of server virtualization has become a standard industry practice. This shift has dramatically improved IT efficiency in companies around the world, benefiting from improved scalability, high availability and greater workload portability. Businesses can now do more with less.

This shift also means that you need a new, scalable and easy to manage approach to get complete visibility into (inter-) VM traffic, in order to monitor for performance, security and availability.

To gain visibility in virtual traffic and forward filtered network traffic to network security and network monitoring tools, you need a Virtual TAP (vTAP).

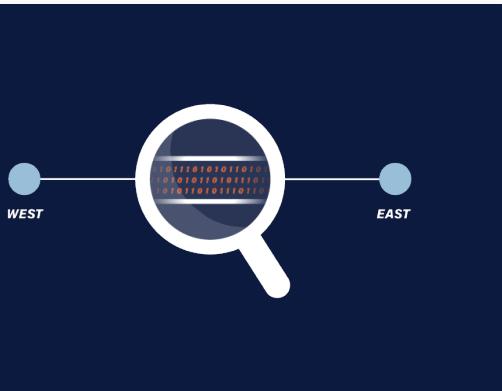
FEATURES

- Enables security, availability, and performance through proactive monitoring of virtual data centers
- Complete visibility of traffic in virtual environments, eliminating blind spots
- Central management interface for a single overview of the entire virtual visibility system
- Filtering helps bring down the virtual traffic to actionable data and prevent network congestion
- Easily scalable
- Forward virtual traffic back into physical network for analysis



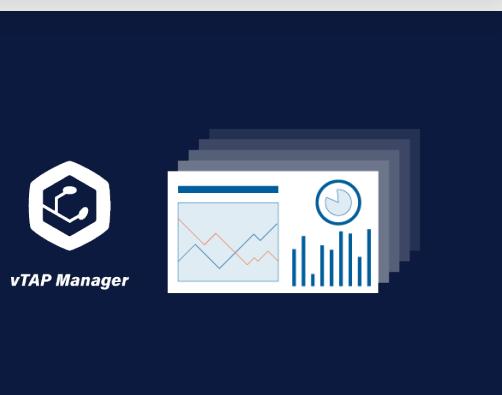
Visit our website and request a quote for more information.

www.profitap.com/vtap ▶



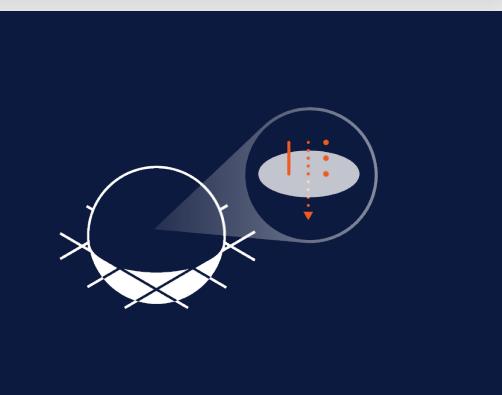
Provide inter-VM traffic visibility

Complete visibility of VM traffic (including inter-VM east-west traffic flows) for security, availability, and performance monitoring.
Profitap vTAP taps directly on the VMware infrastructure, which means no extra privileged access to the hypervisors is required.



Highly scalable orchestrator

The vTAP controller is able to manage visibility of thousands of VMs in a simple and comprehensive way.
Based on your requirements, Profitap vTAP can scale at the click of a button and grow with your network.



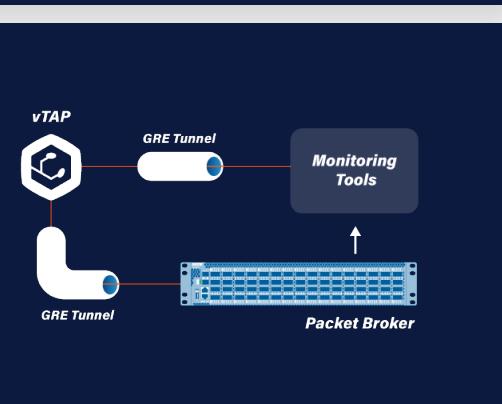
Filter traffic of interest

Flexible filters with L3 and L4 criteria and exclude & include filters can be set up to make efficient use of available bandwidth, ultimately preventing network congestion.
Filtered data can be forwarded to any available interface.



Single pane of glass management

One single interface to manage visibility of all your virtual datacenters. This enables you to set up and manage your virtual monitoring system quickly and easily.



Versatile traffic exporter

Filtered traffic flows of interest can be forwarded to any type of traffic collector, analyzer, located in the same virtual datacenter or remote, as well as Profitap physical Packet Brokers.

MANAGING & OPTIMIZING DATA FLOW

OPTIMIZE DATA FLOW AND MAINTAIN NETWORK FLEXIBILITY

Empower security and performance monitoring tools

Network security breaches and performance issues on critical applications give companies plenty of reasons to monitor their networks. To get a complete overview of the network, there are many points in the architecture where the traffic needs to be accessed; for example: at the client, on the network infrastructure, at the edge, in the data center, and in the cloud.

In many cases, however, this results in many more TAP connections than the monitoring tools can handle. This is where Network Packet Brokers provide an extra layer to the monitoring platform, which helps aggregate and distribute the right traffic to the right tools efficiently.

Network Packet Brokers are placed between the monitoring and security tools and network TAPs or mirror/SPAN ports. They orchestrate the traffic coming from multiple network links and can perform advanced, intelligent traffic management to ensure that monitoring tools receive the appropriate packet data. Deploying a Network Packet Broker adds a layer of intelligence to optimize the monitoring architecture and increase the performance of monitoring and security tools.

Network Packet Brokers help you:

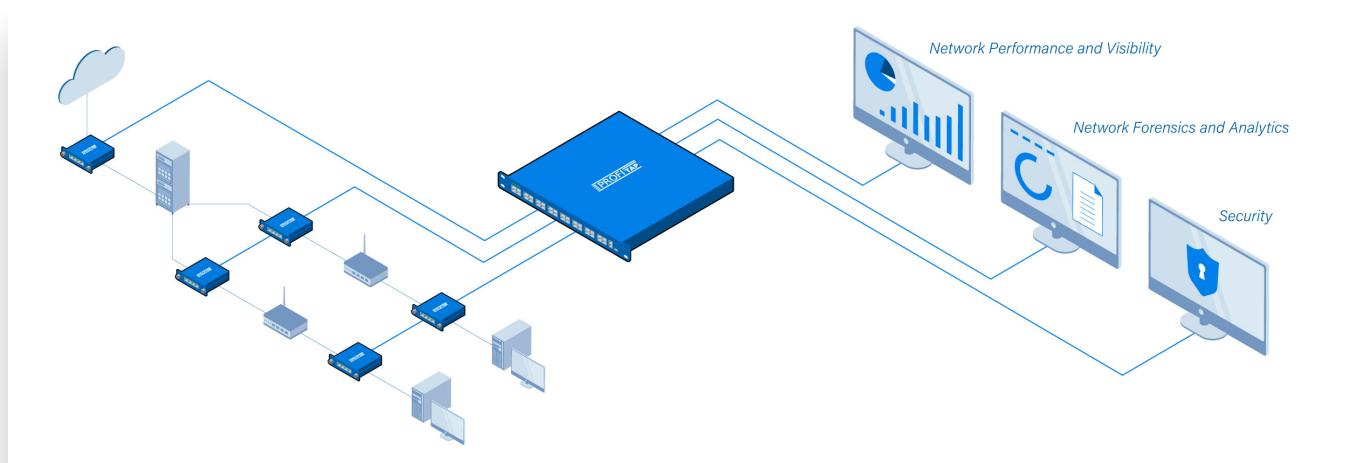
- Obtain complete visibility into your physical and virtual networks.
- Reduce cost and complexity by streamlining data for monitoring and security tools with advanced filtering capabilities.
- Enhance the utilization and productivity of security and monitoring tools for better ROI.
- Easily scale out your network infrastructure with the flexibility to deploy or upgrade your tools efficiently as your network grows.

XX-SERIES NETWORK TRAFFIC AGGREGATORS

AGGREGATION, REPLICATION, LOAD BALANCING, FILTERING

A Network Traffic Aggregator is an entry level Network Packet Broker (NPB) that optimizes traffic flow between TAP and SPAN connections and network monitoring, and security tools. By maintaining a many-to-many (M:M) port mapping of network ports to monitoring ports, they can direct network traffic efficiently. Filters can be applied to optimize bandwidth usage on the network, and load on connected tools, increasing their performance.

Profitap XX-Series Network Packet Brokers are high density packet brokers, bringing you the power and flexibility of network traffic management with a high throughput, in a single 19" RU. All XX-Series Network Packet Brokers offer powerful features, such as aggregation, replication, filtering, and load balancing.



Load Balancing

Balance traffic over multiple monitoring and security tools



Aggregation

Aggregate traffic coming from multiple incoming links



Filtering

Only send actionable data to each of the connected tools



Replication

Replicate traffic to multiple monitoring and security tools

XX series	Interfaces	1G	10G	40G	100G	400G
XX-720G	48 x 10G SFP+ 6 x 40G QSFP+	✓	✓	✓	—	—
XX-1800G	48 x 25G SFP28 6 x 100G QSFP28	✓	✓	✓	✓	—
XX-3200G	32 x 40/100G QSFP28	—	✓	✓	✓	—
XX-12800G	32 x 100/400G QSFP-DD	—	—	✓	✓	✓



XX-720G



XX-1800G



XX-3200G



XX-12800G

Visit our website and request a quote
for more information.

www.profitap.com/network-traffic-aggregators ►

X2-SERIES NETWORK PACKET BROKERS

OPTIMIZE THE PERFORMANCE OF NETWORK ANALYSIS & SECURITY TOOLS

A Network Packet Broker (NPB) is a device that optimizes the flow of traffic between TAP and SPAN connections and network monitoring, security and acceleration tools. By maintaining a many-to-many (M:M) port mapping of network ports to monitoring ports, they can direct network traffic efficiently, and filters can be applied to optimize bandwidth usage on the network. This also means that the performance of out-of-band tools increases as they receive only actionable data.

The Profitap X2-Series NPBs are next-generation network packet brokers (NGNPBs) with a total throughput of up to 6.4 Tbps. In addition to the standard XX-Series features, these NGNPBs offer an extensive set of features, such as packet slicing, GTP IP filtering, ERSPAN tunneling & de-tunneling, packet deduplication, and timestamping.



Packet Slicing

Remove payload that is irrelevant to network monitoring and security analysis, conserving disk space and load on capture devices.



GTP IP Filtering

Filter by IP in GTP sessions based on information contained in the data stream, identifying source and destination.



Timestamping

Leverage accurate timing information for accurate forensic analysis, legal and criminal investigation.



ERSPAN (De)Tunneling

Integrate the X2-3200G as a single, centralized point for ERSPAN stripping in a new or already existent monitoring system based on data ERSPAN encapsulation.



Packet Deduplication

Optimize network efficiency and traffic storage eliminating redundant packet copies.

Packet deduplication license references:

X2-2000G-LIC-D

X2-3200G-LIC-D

X2-6400G-LIC-D

X2 series	Interfaces	1G	10G	40G	100G
X2-2000G	48 x 1/10/25G SFP28 8 x 40/100G QSFP28	✓	✓	✓	✓
X2-3200G	32 x 40/100G QSFP28	—	✓	✓	✓
X2-6400G	64 x 40/100G QSFP28	—	✓	✓	✓



X2-2000G



X2-3200G



X2-6400G

Visit our website and request a quote
for more information.

www.profitap.com/network-packet-brokers ►

X3-SERIES NETWORK PACKET BROKERS

ADVANCED TRAFFIC INTELLIGENCE FOR SECURITY AND PERFORMANCE ANALYSIS

Modern network monitoring and analytics do not only rely on packets. Security and NPM solutions need a complete visibility of the flow context. The pre-treatment layer must understand this context to offer the best-in-class level of traffic optimization.

The new generation of X3-Series Network Packet Brokers enables full visibility over packets and flows, as well as complex advanced processing for extended visibility. The X3-Series are the most versatile Network Packet Brokers, with both simple and very advanced features.



SSL/TLS Decryption

The X3-Series supports in-line and passive SSL/TLS traffic decryption. The TLS decryption feature reduces blindspots that exist with encrypted traffic. The X3-Series supports passive decryption of TLS 1.2 and below. TLS 1.3 in-line decryption is done via a proxy. Decrypted traffic can be sent to an out-of-band security or analysis appliance.



Data Masking

Decrypted traffic can expose confidential data to network engineers and analysts, resulting in security or privacy implications. The X3-Series can obfuscate sensitive data to comply with regulations and prevent data leakages. Data masking enables complete visibility into decrypted data without the risk of exposing sensitive data.



Deduplication

With TAPs and mirror ports at multiple points inside the network, the same network data may be captured multiple times, causing duplicate packets inside the monitoring system.

Sending unnecessary duplicate packets to analysis and security tools significantly impacts their performance. The X3-Series can dynamically discard duplicated packets before they are sent out.

Thanks to the large time window for packet comparison and extensive configurability of the deduplication feature, the X3-Series can mitigate multiple sources of duplicate packets, like network design flaws or switch SPAN ports.



NetFlow v5/v9 Export

NetFlow is an efficient protocol for providing information about network traffic and utilization to analysis tools. X3-Series network packet brokers can act as flow exporters, processing and sending flow data to flow collectors.

Implementing NetFlow on devices like routers and switches can impact their performance. Instead, setting up X3-Series packet brokers as flow exporters allows such devices to focus their processing power on their primary functions.

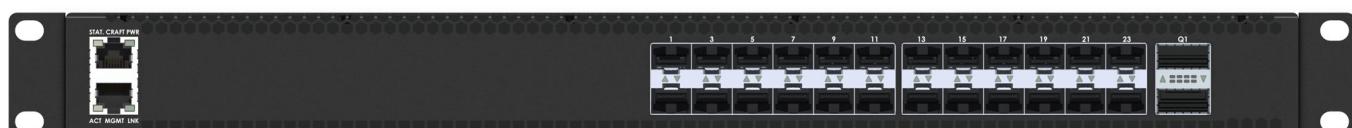
X3 series	Type	Interfaces	1G	10G	40G	100G
X3-880G	Advanced Network Packet Broker	48 x 1/10G SFP+ 4 x 40/100G QSFP28	✓	✓	✓	✓
X3-440G	Advanced Network Packet Broker	24 x 1/10G SFP+ 2 x 40/100G QSFP28	✓	✓	✓	✓
X3-880G-ID	SSL/TLS In-Line Decryption	48 x 1/10G SFP+ 4 x 40/100G QSFP28	✓	✓	✓	✓
X3-440G-ID	SSL/TLS In-Line Decryption	24 x 1/10G SFP+ 2 x 40/100G QSFP28	✓	✓	✓	✓
X3-880G-GC	GTP Traffic Correlation	48 x 1/10G SFP+ 4 x 40/100G QSFP28	✓	✓	✓	✓
X3-440G-GC	GTP Traffic Correlation	24 x 1/10G SFP+ 2 x 40/100G QSFP28	✓	✓	✓	✓

Feature highlights

- SSL/TLS decryption
- Data masking
- Packet deduplication
- TCP packet reordering and fragments re-assembling
- Full tunneling capability
- Packet Slicing
- IMSI Filtering / Correlation
- GTP Traffic Correlation (GTP model)
- Timestamping
- Export NetFlow v5/v9
- L2-L7 Filtering, DPI
- Load Balancing
- Any-to-any Replication and Aggregation
- Microburst Protection



X3-880G



X3-440G

Visit our website and request a quote
for more information.

www.profitap.com/network-packet-brokers ►

NPB MANAGEMENT

XX, X2 and X3-Manager are web-based interfaces that allow the user to configure and monitor the behavior of a Profitap Network Packet Broker. These interfaces are based on a web application, allowing users to easily access them from any OS or platform.

- ▶ Full control over 1GbE, 10GbE, 25GbE, 40GbE and 100GbE network traffic for monitoring thanks to the intuitive GUI.
- ▶ Multiple filter rules per port in any combination for various routing, filtering, duplication or replication and many more options can be configured by the GUI to allow instant adaptation to all kind of analysis.
- ▶ Storage of multiple rule set configurations that allow instant rule set changes to ease meeting the current requirements.



Information

System	
Media Version	X2-3200G
Hardware Revision	1.0
Software Revision	v0.13.2
Serial Number	[REDACTED]
Admin Name	Profitap HQ BV
Admin Phone	+31...
Admin E-mail	support@profitap.com

Date and Time	
Date	29/06/2023
Time	15:03:12
Timezone	Etc/UTC
Uptime	2D - 4h - 53m - 13s

Global Received	
Received Bandwidth	23.40 Gbps
Received Octets All	276,419,209,845,812
Received Octets Good	276,419,209,813,954
Received Frame All	340,074,358,666
Received Frame Good	340,074,358,621
Received Frame Error	0
Received Frame Unsorted	48,930,607,847

Sensors	
System Status	WARNING
CPU Temperature	72.00 °C / 161.60 °F
System Temperature	69.00 °C / 157.78 °F
Air Temperature	51.00 °C / 123.91 °F
FAN 1 Status	FUNCTIONAL
FAN 2 Status	FUNCTIONAL
FAN 3 Status	FUNCTIONAL
FAN 4 Status	FUNCTIONAL

Asset Information

Asset Name	Profitap
Asset Code	PFT-6556AG
Building	HTC24
Address	High Tech Campus
City	Eindhoven
Region	NL
Country	NL

Network

MAC Address	[REDACTED]	Hostname	x2-profitap
IPv4 Address	[REDACTED]	IPv4 Address	[REDACTED]
IPv4 Gateway	[REDACTED]	IPv4 Gateway	[REDACTED]
IPv4 DNS 1	[REDACTED]	IPv4 DNS 1	[REDACTED]
IPv4 DNS 2	[REDACTED]	IPv4 DNS 2	[REDACTED]

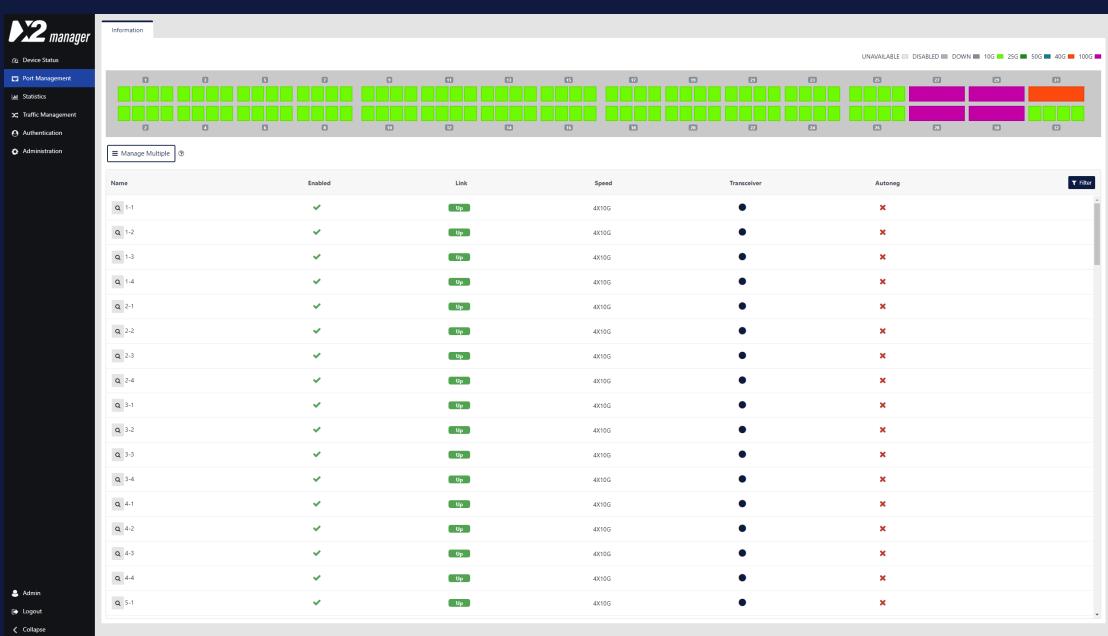
Global Transmitted

Transmitted Bandwidth	40.36 Gbps
Transmitted Octets All	587,277,675,727,050
Transmitted Octets Good	587,277,675,659,356
Transmitted Frame All	722,000,023,403
Transmitted Frame Good	722,000,023,314
Transmitted Frame Error	0
Buffer Frame Drop	0

Temperatures

Device Status

Device status offers a quick overview of operational statistics related to the packet broker hardware. Measured temperatures are recorded with a history of 72 hours, to allow filtering back in time on temperature statistics.



Port Management

Port management offers instant overview of port status and speed. Users control the configuration of all QSFP modules, where each module offers additional information in the specific status section.



Port Statistics

Port statistics displays and monitors the statistics counter for each of the device interfaces. Users can view or export this information for a later analysis. It is also possible to easily compare the traffic bandwidth on each port.

SUPERVISOR

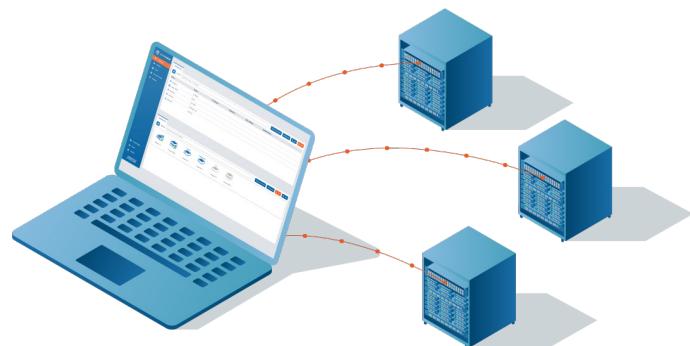
SINGLE PANE OF GLASS NPB FABRIC MANAGEMENT AND CONTROL

Profitap Supervisor is a centralized management system that allows you to organize and control all XX-Series and X2-Series Network Packet Brokers deployed inside your network architecture. It provides a comprehensive overview of the connected monitoring fabric and brings this together into a single interface. Instead of maintaining each device separately, Supervisor helps orchestrate clusters of devices all at once.

By automating update and maintenance processes, Profitap Supervisor simplifies the workflow of managing your network monitoring infrastructure, saving you valuable time and money.

FEATURES

- ▶ At a glance supervision of all connected devices
- ▶ Centralized deployment of firmware updates
- ▶ Simplified tool orchestration workflow
- ▶ Organization of devices and statistics in clusters
- ▶ Easy device access with credential logging



ORDERING INFORMATION

ORDER REFERENCE	DESCRIPTION
SFM-10	Supervisor Fabric Manager, 10 Nodes
SFM-25	Supervisor Fabric Manager, 25 Nodes
SFM-50	Supervisor Fabric Manager, 50 Nodes
SFM-100	Supervisor Fabric Manager, 100 Nodes
SFM-250	Supervisor Fabric Manager, 250 Nodes
SFM-500	Supervisor Fabric Manager, 500 Nodes

TRAFFIC CAPTURE & ANALYSIS

ACCELERATE INCIDENT RESPONSE AND TROUBLESHOOTING
PERFORMANCE

OBSERVE. IDENTIFY. RESOLVE.

Traffic capture and analysis are essential for a wide range of analytics and forensic needs, from application performance monitoring to security threat detection and investigation. Hardware and software solutions for traffic capture and analysis come in many shapes and sizes. Traffic capture and analysis on a single low bandwidth connection between a desktop and a switch is relatively easy to accomplish, but hundreds of high speed connections inside a data center require a different approach and budget.

Network infrastructures are evolving, which shows particularly in the rise of distributed networks. Data centers are migrating to the cloud, to which branch offices around the globe are connected, and to which staff needs the ability to connect in order to work remotely. When selecting the right tool for the job, it is important to start distilling the monitoring reason, and the locations in the infrastructure at which key capture points are required to get the right data at the right time. Whether it is in the data center, a part of a building, a whole campus, or a branch office, a well implemented traffic capture and analysis solution helps track down performance and security issues in the least amount of time possible, keeping the business secure and performant.

Traffic capture and analysis tools enable you to:

- ◎ Acquire full network and application visibility at key monitoring points.
- ◎ Quickly identify and resolve network and application issues.
- ◎ Perform both real-time and historical data investigation for forensic analysis.
- ◎ Optimize the performance and security of your business-critical networks and applications.

PROFISHARK

COMPLETE VISIBILITY OF YOUR ENTIRE NETWORK ANYTIME, ANYWHERE

ProfiSharks are portable traffic capture devices that provide quick packet-level insight anywhere they are deployed. With capture regardless of packet rate and high quality hardware timestamping, ProfiShark delivers high fidelity capture files, forming an ideal starting point for troubleshooting or network forensics. Designed for easy, non-intrusive traffic capture, ProfiShark offers a valuable improvement over less performant options, such as SPAN ports on a switch or direct capture on a laptop. They give reliable insight into the network, ensuring the quality of analysis, and optimizing workflow, without dropping any packets.

Connected via USB to a host PC or laptop, in-line or out-of-band traffic can be forwarded directly to packet analyzer software, like Wireshark, or stored to disk. To ensure optimum network protection, the monitored network is physically separated from the management interface. The capture control and hardware settings can be managed via the included ProfiShark Manager application.



Quickly get packet-level insights

ProfiShark enables complete data capture in a portable form factor. This means you can deploy rapidly anywhere, and capture the traffic data you need, with no performance impact on your production network.

Get transparent and non-intrusive access

Capture network data without impacting security or performance. The ProfiShark and host PC will not show up as a node on the network. Network connection is maintained, even when power to the ProfiShark is disconnected. ProfiShark is set up to passthrough PoE.

Get the timestamp accuracy you need

Accurate timestamping is essential for the analysis of performance metrics like TCP flow throughput, delay, and jitter. ProfiShark offers models with down to 5ns hardware timestamping, and advanced GPS/PPS timestamping features on the + models.

Get trace files you can rely on

To help optimize your analysis workflow and consume less disk storage, ProfiShark offers packet slicing capabilities, making sure you only get actionable data.



PROFISHARK 1G



PROFISHARK 10G

The ProfiShark 1G and 10G can capture any traffic, frames of any size and type, in-line or SPAN, for analysis and monitoring with Wireshark, or any major software analyzer. The included ProfiShark Manager software provides additional information, statistics, and configuration and capture options.



PROFISHARK 1G+



PROFISHARK 10G+

The ProfiShark 1G+ and 10G+'s GPS/GLONASS function can tag packets with accurate UTC timestamps. The ProfiShark 1G+ and 10G+ can also receive or generate a PPS signal, enabling accurate timestamp synchronization in various topologies.



PROFISHARK 100M

The ProfiShark 100M is designed for the capture of 10/100M Ethernet traffic. It is the perfect tool for troubleshooting Real-Time Industrial Ethernet protocols. This pocket-sized portable traffic capture device gives you all the flexibility and ease of use you require for the monitoring of industrial networks.



Long-term Traffic Capture

ProfiShark long-term capture solution is designed with flexibility in mind. Combined with a NAS for storage tailored to your specific needs, the long-term capture feature makes it easy to catch intermittent problems in the act.



Model	Speed	Net Input(s)	TAP output(s)	Additional connectors	Dimensions (WxDxH)
	C1AP-100	10/100 Mbps	2 x RJ45	1 x USB 3.0	Optional 5 VDC input 69 x 124 x 24 mm 2.72 x 4.88 x 0.94 in
	C1AP-1G	10/100/1000 Mbps	2 x RJ45	1 x USB 3.0	Optional 5 VDC input 69 x 124 x 24 mm 2.72 x 4.88 x 0.94 in
	C1AP-1G2	10/100/1000 Mbps	2 x RJ45	1 x USB 3.0 1 x SMA female (PPS) 1 x SMA female (GPS) 1 x 5 VDC optional input	105 x 124 x 26 mm 4.13 x 4.88 x 1.02 in
	C1AP-10G	1/10 Gbps	2 x SFP/SFP+	1 x USB 3.0	Optional 5 VDC input 105 x 124 x 26 mm 4.13 x 4.88 x 1.02 in
	C1AP-10G2	1/10 Gbps	2 x SFP/SFP+	1 x USB 3.0 1 x SMA female (PPS) 1 x SMA female (GPS) 1 x 5 VDC optional input	105 x 124 x 26 mm 4.13 x 4.88 x 1.02 in

System Requirements:

- ⦿ Dual Core Processor
- ⦿ 4 GB memory
- ⦿ USB 3.0 port

Supported OS:

- ⦿ Windows 7/8/10 (32/64 bit)
- ⦿ Linux
- ⦿ macOS

Visit our website and request a quote for more information.

www.profitap.com/profisshark-network-taps ►



ALL-IN-ONE NETWORK TRAFFIC MONITORING SOLUTION

IOTA is a powerful network capture and analysis solution for edge and core networks. The IOTA lineup consists of portable EDGE models, high-speed CORE models, and the IOTA CM centralized device management system.

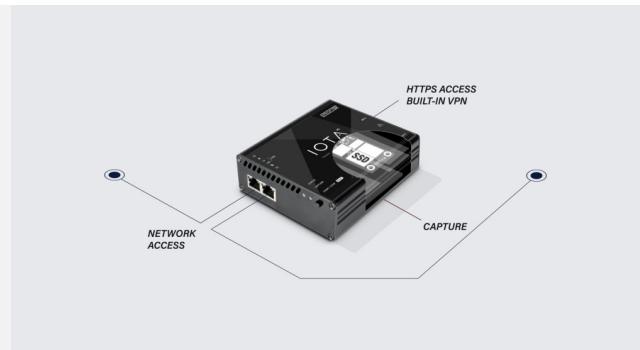
Altogether, the IOTA solution provides fast and efficient network analysis and troubleshooting capabilities to branch offices, SME businesses, and core networks, such as data centers.

IOTA allows you to capture network traffic without affecting network performance or security and gives detailed real-time and historical network traffic visibility into critical applications and data. IOTA helps quickly resolve network issues like performance and application problems through complete packet and metadata analysis.



Monitor key network metrics and performance indicators

- Monitor hosts, top talkers, bandwidth, latency, TCP, UDP, IPv4, IPv6, VLAN, DNS, and many more at a glance using a set of comprehensive dashboards.
- Keep a close eye on the most essential performance metrics, retransmissions, packet loss, latency, throughput, availability, connectivity, and more.
- Full visibility into 200+ applications and protocols (DNS, HTTP, SSH, Office 365, Skype, WhatsApp, Netflix, etc.).



TAP, capture and analyze network traffic with a single box

- IOTA captures high-fidelity PCAP traces to an internal SSD, from which metadata is extracted, allowing for a quick and responsive search in the dashboards.
- Real-time and historical network analysis: Explore long-term datasets accumulated over days, weeks, or months.
- Fully managed over HTTPS and with a built-in VPN, IOTA offers easy deployment and usage.

SOLUTION OVERVIEW

IOTA EDGE



Small/mid-size enterprises, small branches, and small data centers

- Dedicated and portable deployment scenarios
- In-line or out-of-band
- 1 TB or 2 TB capture storage
- Capture performance 3.2 Gbps

IOTA CORE



Core networks, large branches, and data centers

- Dedicated deployment on central capture point
- Out-of-band
- 4, 8 or 16 TB capture storage
- Capture performance 20 Gbps

IOTA CM



Centralized management application

- Central interface for bird's-eye view insight into IOTA analytics
- Fleet management and maintenance
- Multi-segment analysis: Latency measurement between different capture points for edge IOTAs

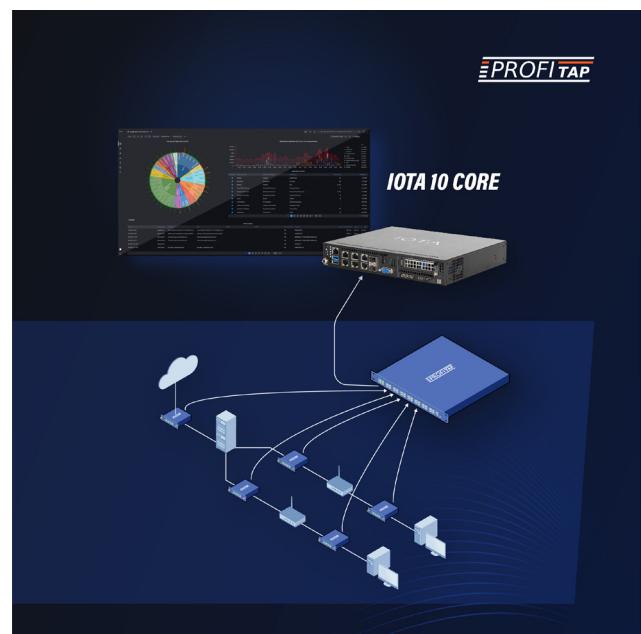
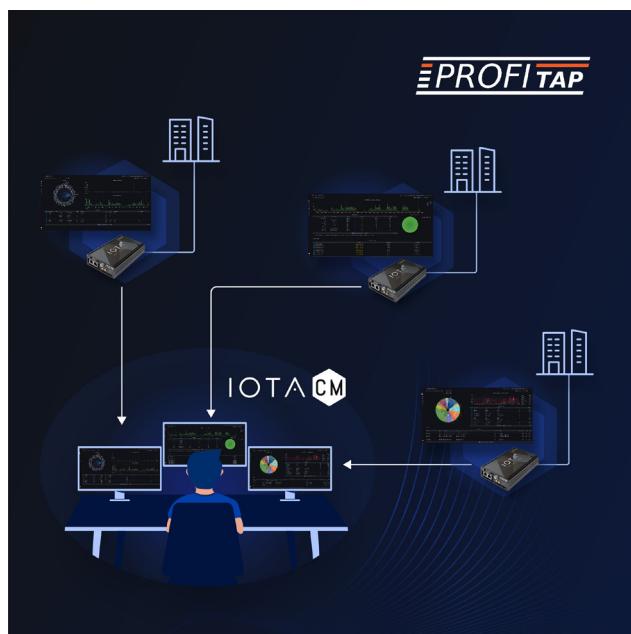
DEPLOYMENT SCENARIOS

Retail/branch office

Monitor individual IOTA EDGE and CORE capture points or centrally through IOTA CM.

Data center deployment

Access and optimize network traffic through TAPs and Network Packet Brokers, centrally collecting it in a IOTA CORE model.



IOTA MODEL COMPARISON

IOTA EDGE

Model	Use Case	Network Connectors	Timing Connectors	Internal Storage	Power	Rack-mounted	Integrated Analysis Dashboards
 IOTA 1G	Key capture point / Remote office	2 x 10M/100M/1G RJ45 in-line/SPAN	-	1 TB SSD	12 VDC or 24-48 VDC (industrial)	-	<input checked="" type="checkbox"/>
 IOTA 1G+	Key capture point / Remote office	2 x 10M/100M/1G RJ45 in-line/SPAN	1 x SMA female (PPS) 1 x SMA female (GPS)	1 TB or 2 TB swappable SSD	12 VDC or 24-48 VDC (industrial)	-	<input checked="" type="checkbox"/>
 IOTA 10G	Large branch / WAN edge	2 x 1G/10G SFP+ in-line/SPAN	-	1 TB SSD	12 VDC or 24-48 VDC (industrial)	-	<input checked="" type="checkbox"/>
 IOTA 10G+	Large branch / WAN edge	2 x 1G/10G SFP+ in-line/SPAN	1 x SMA female (PPS) 1 x SMA female (GPS)	1 TB or 2 TB swappable SSD	12 VDC or 24-48 VDC (industrial)	-	<input checked="" type="checkbox"/>
 IOTA 1G M12	Industrial networks	2 x 10M/100M/1G M12 X-Coded	-	1 TB SSD	12 VDC or 24-48 VDC (industrial)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 IOTA 1G	Key capture point / Remote office	2 x 10M/100M/1G RJ45 in-line/SPAN	-	1 TB SSD	12 VDC or 24-48 VDC (industrial)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 IOTA 1G+	Key capture point / Remote office	2 x 10M/100M/1G RJ45 in-line/SPAN	1 x SMA female (PPS) 1 x SMA female (GPS)	1 TB or 2 TB swappable SSD	12 VDC or 24-48 VDC (industrial)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 IOTA 10G	Large branch / WAN edge	2 x 1G/10G SFP+ in-line/SPAN	-	1 TB SSD	12 VDC or 24-48 VDC (industrial)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 IOTA 10G+	Large branch / WAN edge	2 x 1G/10G SFP+ in-line/SPAN	1 x SMA female (PPS) 1 x SMA female (GPS)	1 TB or 2 TB swappable SSD	12 VDC or 24-48 VDC (industrial)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

IOTA CORE

Model	Use Case	Network Connectors	Timing Connectors	Internal Storage	Power	Rack-mounted	Integrated Analysis Dashboards
 IOTA 10 CORE	Large branches / Core network	2 x 100M/1G RJ45 2x 1/10G RJ45 2 x 10G SFP+	-	4, 8 or 16 TB SSD	12 VDC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

IOTA CM

ENHANCED IOTA ANALYTICS AND CENTRALIZED DEVICE MANAGEMENT

Bring all IOTA analytics together in a single pane of glass

IOTA CM is an application for centralized management of IOTA EDGE and CORE devices. Bringing together analytics from all IOTA capture points into a single interface, network administrators can centrally maintain a fleet of IOTA devices and perform advanced measurements, such as multi-segment analysis between capture points.

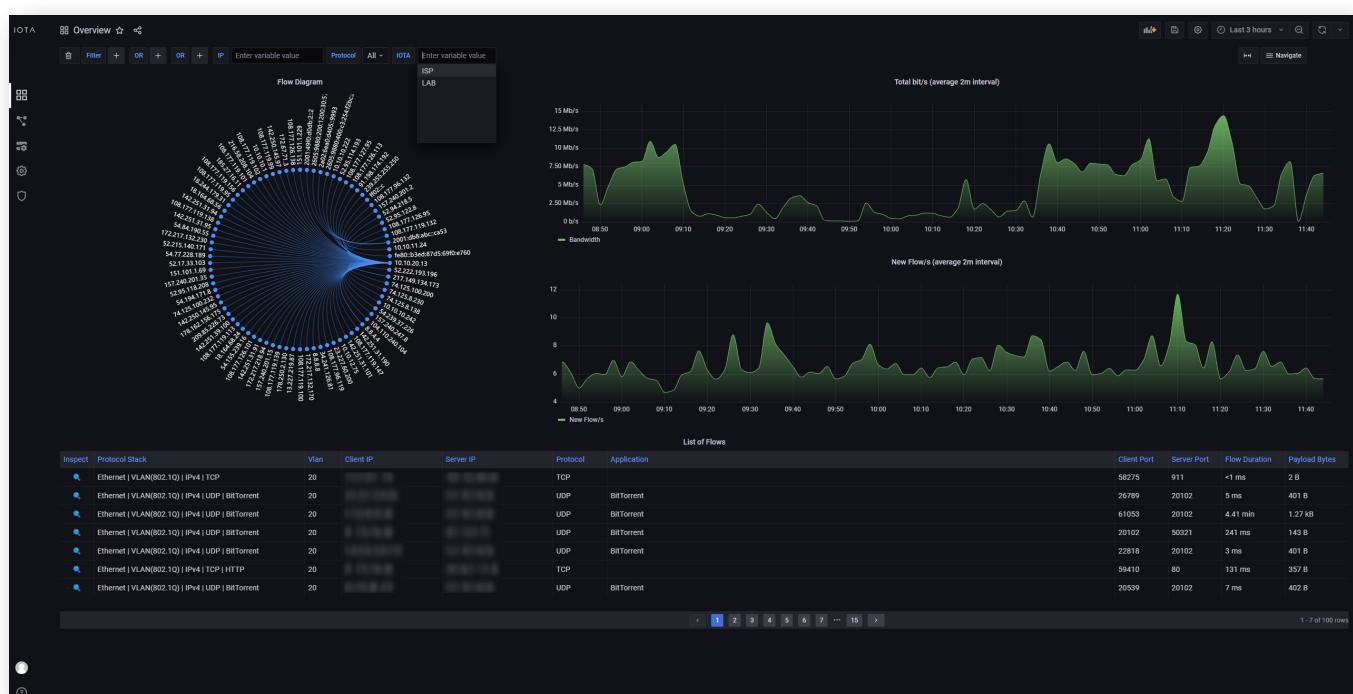
All IOTA devices capture network traffic locally. IOTA CM pulls metadata from all connected IOTA devices, giving insight into performance metrics from each capture segment and allowing you to get a holistic view of the network and compare specific capture locations for further analysis.

IOTA CM overview

- Easy device fleet management and maintenance
- Single viewpoint of metadata collected by all IOTA devices
- Compare metadata from different capture points in a single dashboard
- Multi-segment analysis: latency measurement between different capture points for edge IOTAs



- At-a-glance supervision of connected devices
- Centralized deployment of firmware updates
- Container-based deployment for flexible integration in any modern infrastructure



REAL TIME TRAFFIC ANALYSIS

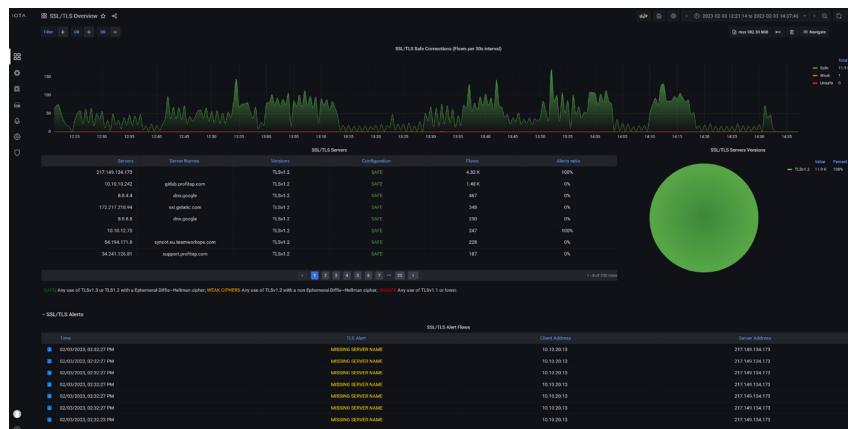
Out of the box, IOTA comes with its own integrated software to help analyze the captured data in real-time. By extracting metadata from the captured files, IOTA is able to give you a real-time visual overview of what is happening on your network. IOTA dashboards help you filter large amounts of network traffic instantly, greatly optimizing your workflow and reducing time spent on troubleshooting.

A selection of available dashboards:



HOME DASHBOARD

A quick overview of Top Talkers and client-server data transfers.



TCP ROUND TRIP TIME

RTT triggers per flow, server, and client. TCP flag statistics.



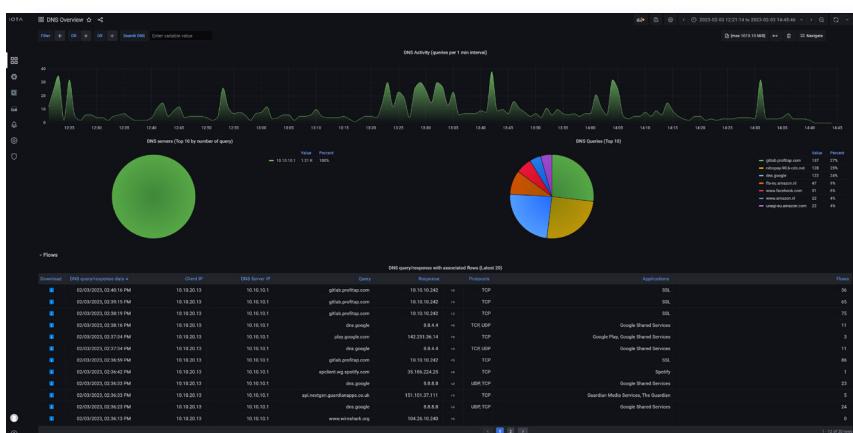
USER EXPERIENCE APPLICATION LATENCY

Application latency from the client IP perspective.



TCP SERVER CONGESTION

An overview of zero windowing events per server over time, detecting when a server is saturated. Includes statistics of number of flows per server.



TCP OUT-OF-ORDER AND LOST PACKETS

Analyze application and network traffic based on Flow ID, Client IP, Server IP, Protocol, etc.



Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products to set new standards in an industry where the definition of excellence is constantly being challenged.

With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 84
5656AG EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

profitap-international

@Profitap

Profitap

Profitap HQ B.V.

The information in this guide is not guaranteed to be complete, and may contain technical or typographical errors. Profitap assumes no responsibility for any inaccurate information in this guide.