PROFITAP
DEEP NETWORK OBSERVABILITY

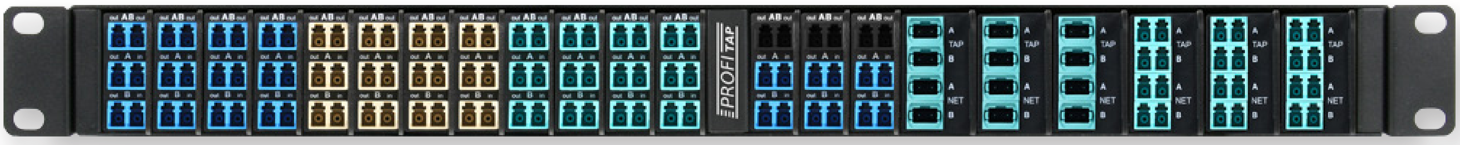
INTRODUCTION TO TAPs

Creating a robust network monitoring system with network TAPs

Network performance and security analysis without impacting operational network performance

TAPs are hardware devices strategically placed at key locations within the network infrastructure, such as routers, switches, or firewalls, where data access is necessary for monitoring or troubleshooting purposes. To leave no stone unturned, in virtual environments, a virtual TAP, or vTAP, can be installed on virtualized servers, providing comprehensive access and visibility into the east-west traffic flows.

While there are various methods to capture packets on a live network, such as SPAN port forwarding, they often come with significant drawbacks, such as packet loss, out-of-order packets, and the potential for man-in-the-middle attacks. These issues directly impact the quality of analysis and the network's overall security. To address this, it is considered a best practice to deploy network TAPs (Test Access Points) for accessing network traffic.



What is a TAP

A network TAP is a device placed in-line at key capture points in a network. It provides an exact copy of the network traffic passing through it to analysis and monitoring tools.

While there are other solutions on the market, TAPs deliver the best reliability and traffic capture fidelity to support network analysis teams.

The quality of your analysis depends on the quality of the data you capture.

Who needs TAPs

- Organizations who need 24/7 monitoring capabilities (network performance, security analysis, VoIP monitoring, lawful interception).
- Organizations who need easy monitoring access for SLA upkeep.
- Organizations who require an exact copy of network traffic for forensics and legal purposes.
- Organizations who need to conduct troubleshooting without affecting existing switch configuration.

Why use TAPs

- Access to the traffic at key capture points of the network without affecting the network links.
- TAPs are dedicated tools that deliver an exact copy of traffic at line rate without dropping packets.
- Standard fiber TAPs are fully passive, unpowered, introducing no point of failure to the network.
- Copper TAPs are passive in that they do not affect the network traffic and incorporate fail-safe systems.
- TAPs are physical layer devices, separate from the production network, requiring no processing power or port usage on switches, unlike SPAN or port mirroring.
- They can be used in conjunction with network packet brokers for distribution of the monitored traffic to the appropriate tools.
- Data Diodes built into TAPs ensure traffic can only flow in one direction, adding an extra layer of security.
- Meet compliance and regulation standards, such as NIS2 and ANSSI.

Benefits of Profitap TAPs

Copper TAPs

- Fail-safe design: provide an exact copy of the network traffic without introducing single points of failure in the network.
- No alteration of traffic on the network link: monitoring ports physically separated from the network.
- No Break Technology ensures low failover time, reducing the chances of Spanning Tree reconvergence.
- Link-Failure Propagation transmits link failure errors between ports, allowing the network to activate a redundant path, ensuring less downtime in high availability networks.

Fiber TAPs

- Fully passive, unpowered, making them inherently fail-safe and non-intrusive, guaranteeing a permanent network link at all times.
- High level of quality control, low insertion loss.
- Various fiber types and split ratios available.
- MOD-TAP modular system is flexible and scalable: combine different fiber types and speeds in a single chassis.

Aggregation TAPs

- You can aggregate lower speed links to higher speed switches or packet brokers to optimize port usage.
- You can monitor traffic from multiple links with a single tool.
- Increase lifespan of existing analysis and monitoring tools by optimizing port usage.
- It's possible to convert media type going from the TAP point to a different type on the output, matching your input on the monitoring tools.
- VLAN tagging provides physical link/port reference of aggregated packets, to track which link the packets originated from.

Secure TAPs

- 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 and into the operational network.
- Secured firmware implemented on active TAPs cannot be read or altered by 3rd parties, ensuring the safe operation of the devices.
- Tamper-evident security seals prevent unnoticed opening and tampering of the devices.
- Randomized patterns used on seals and packaging to ensure secured logistics.

Data Diode TAPs

- DiodeTAP fiber modules feature an optical data diode, which prevents accidental or malicious light insertion from the monitor ports and into the production network.
- Copper TAPs physically isolate the monitoring outputs from the operational network, blocking all data transmission from TAP to NET, while providing full data connectivity from NET to TAP.

Regeneration/Replication TAPs

- Output multiple copies of the traffic from a single TAP point.
- Regeneration Fiber TAPs regenerate the optical signal to mitigate the power reduction that results from splitting.

Bypass TAPs

- Deployed together with in-line security tools to ensure optimal uptime of critical network segments.

vTAP

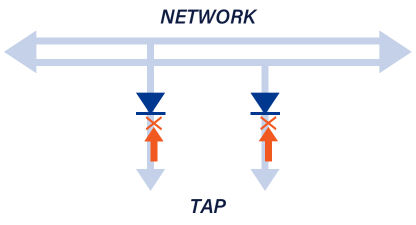
- Monitor traffic in virtualized environments and forward it to physical or virtual monitoring tools.

Virtual TAP

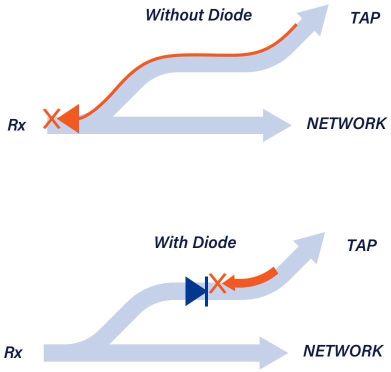
A virtual TAP is a software solution designed for monitoring network traffic in virtual environments, i.e. VM (Virtual Machine) and inter-VM traffic. Profitap vTAP deploys virtual tapping points and virtual Network Packet Brokers based on user requirements, to copy, filter, and forward traffic of interest to physical or virtual monitoring tools.

Data Diode

The Data Diode function present in our Diode Fiber TAP (F1D-MOD) and Copper TAPs prevents any accidental or malicious insertion of signal coming from the monitor ports from entering and disrupting the operational network. Data Diode adds an extra layer of security in deployments with security and monitoring tools.



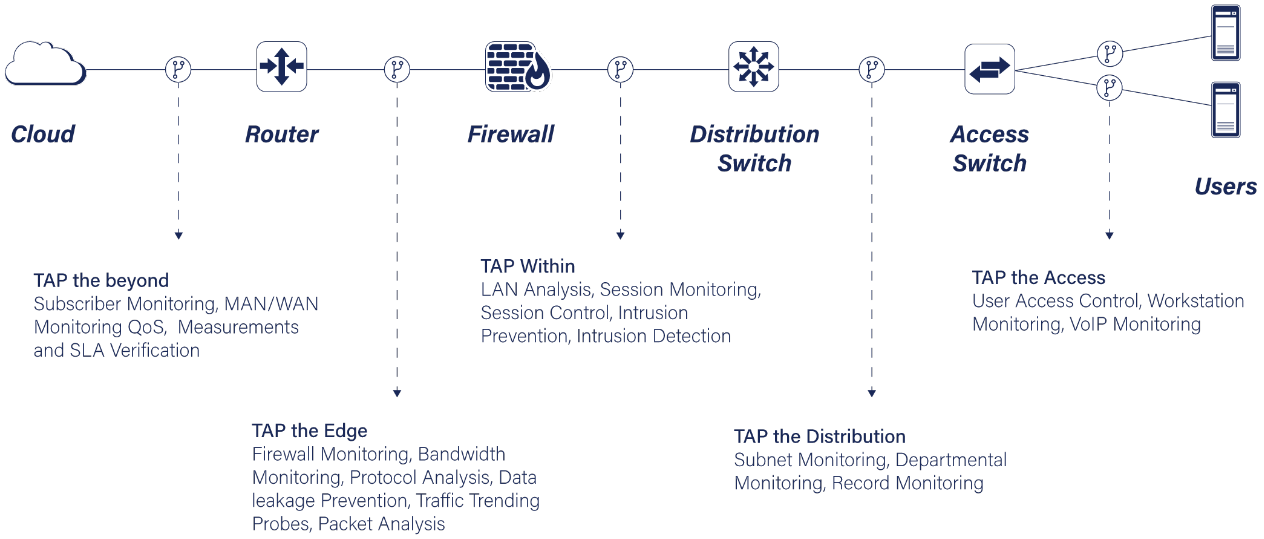
Copper TAP Data Diode



Fiber TAP Data Diode

Where to place TAPs

TAPs are typically placed at critical points of the network where network analysts need traffic visibility. Depending on the monitoring objective, this can be anywhere in the network. The illustration below gives more information on specific capture points.



TAP the beyond
Subscriber Monitoring, MAN/WAN Monitoring QoS, Measurements and SLA Verification

TAP the Edge
Firewall Monitoring, Bandwidth Monitoring, Protocol Analysis, Data leakage Prevention, Traffic Trending Probes, Packet Analysis

TAP Within
LAN Analysis, Session Monitoring, Session Control, Intrusion Prevention, Intrusion Detection

TAP the Distribution
Subnet Monitoring, Departmental Monitoring, Record Monitoring

TAP the Access
User Access Control, Workstation Monitoring, VoIP Monitoring

Profitap Network TAPs

Product reference	Type	Speed	Network links*	Monitor outputs*	Port types
C1R-100	Copper	10/100 Mbps	1	1	RJ45 8-pin 10/100 Mbps
C20-100	Copper	10/100 Mbps	20	20	RJ45 8-pin 10/100 Mbps
C1R-1G	Copper	10/100/1000 Mbps	1	1	RJ45 8-pin 10/100/1000 Mbps
C1R-1G-S (secure TAP)	Copper	10/100/1000 Mbps	1	1	RJ45 8-pin 10/100/1000 Mbps
C8-1G	Copper	10/100/1000 Mbps	8	8	RJ45 8-pin 10/100/1000 Mbps
C8-1G-S (secure TAP)	Copper	10/100/1000 Mbps	8	8	RJ45 8-pin 10/100/1000 Mbps
C1-1G-RG2	Copper	10/100/1000 Mbps	1	2	RJ45 8-pin 10/100/1000 Mbps
C1R-10G	Copper input, SFP output	10M/100M/1G/10G	1	1	Net: RJ45 8-pin 10M/100M/1G/10G Tap: SFP+
F1L-MOD	Fiber	1–400 Gbps	1	1	LC SM 9µm, MM 50µm, MM 62.5µm Split ratio: 50/50, 60/40, 70/30
F1D-MOD (DiodeTAP)	Fiber	1–400 Gbps	1	1	LC SM 9µm, MM 50µm Split ratio: 50/50, 60/40
F1B-MOD	Fiber	40/100 Gbps	1	1	LC OM4 MM 50µm, OM5 MM 50µm Split ratio: 50/50
F1M-MOD	Fiber	40/100/400 Gbps	1	1	MTP MM SR4, MM SR8, MM SR10, SM PLR4, SM PSM4 Split ratio: 50/50, 70/30
F1RL	Fiber	1–100 Gbps	1	1	LC SM 9µm, MM 50µm, MM 62.5µm Split ratio: 50/50, 60/40, 70/3
F4L	Fiber	1–100 Gbps	4	4	LC SM 9µm, MM 50µm, MM 62.5µm Split ratio: 50/50, 60/40, 70/30
F8L	Fiber	1–100 Gbps	8	8	LC SM 9µm, MM 50µm, MM 62.5µm Split ratio: 50/50, 60/40, 70/30
F1x3L	Fiber	1–100 Gbps	1	2	LC SM 9µm, MM 50µm Split ratio: 50/25/25, 40/30/30
F1R-40BD	Fiber	40/100 Gbps	1	1	LC OM4 MM 50µm, OM5 MM 50µm Split ratio: 50/50
F3R-40BD	Fiber	40/100 Gbps	3	3	LC OM4 MM 50µm, OM5 MM 50µm Split ratio: 50/50
F1L-AT	Fiber	1/10 Gbps	1	1	LC SM 9µm, MM 50µm
F1L-RG2	Fiber	1/10 Gbps	1	2	LC SM 9µm, MM 50µm
F1L-RG4	Fiber	1/10 Gbps	1	4	LC SM 9µm, MM 50µm

C8R-X1	Copper input, SFP output	10/100/1000 Mbps	4	1	Net: RJ45 8-pin 10/100/1000 Mbps Tap: SFP+ 1/10 Gbps
C8R-X2	Copper input, SFP output	10/100/1000 Mbps	4	2	Net: RJ45 8-pin 10/100/1000 Mbps Tap: SFP+ 1/10 Gbps
F8R-X1	SFP	10/100/1000 Mbps	8 out-of-band connections	1	Net: SFP 10/100/1000 Mbps Tap: SFP+ 1/10 Gbps
F8R-X2	SFP	10/100/1000 Mbps	8 out-of-band connections	2	Net: SFP 10/100/1000 Mbps Tap: SFP+ 1/10 Gbps
F1-10G-BP	Fiber input, SFP output	1/10 Gbps	1	1	Net: LC SM 9µm or LC MM 50µm Tap: SFP+ 1/10 Gbps
F1-40G-BP	Fiber input, SFP output	40 Gbps	1	1	Net: LC SM 9µm or MPO MM 50µm Tap: QSFP+ 40 Gbps
F4-10G-BP	Fiber input, SFP output	4 x 10 Gbps	4	4	Net: MPO SM 9µm or MPO MM 50µm Tap: QSFP+ 40 Gbps

* These refer to logical links and logical monitor outputs. The number of physical ports this corresponds to depends on the type of connection. For a standard full-duplex copper TAP (e.g. C1R-1G), 1 link consists of 2 ports, and 1 monitor output consists of 2 ports (one per direction). For a standard LC fiber TAP (e.g. F1RL, F1L-MOD), 1 link consists of 4 ports (2 x LC duplex), and 1 monitor output consists of 2 ports (one per direction).