

SOFTPROM

PROFITAP

*ПРОЗРАЧНОСТЬ ВАШЕЙ СЕТИ.
В ЛЮБОЕ ВРЕМЯ. В ЛЮБОМ МЕСТЕ.*

Александр Кобец
Менеджер по развитию бизнеса
+38 (096) 798-78-02
kobets@softprom.com

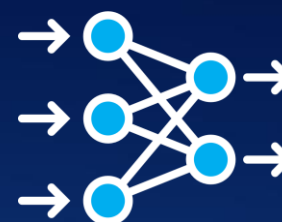
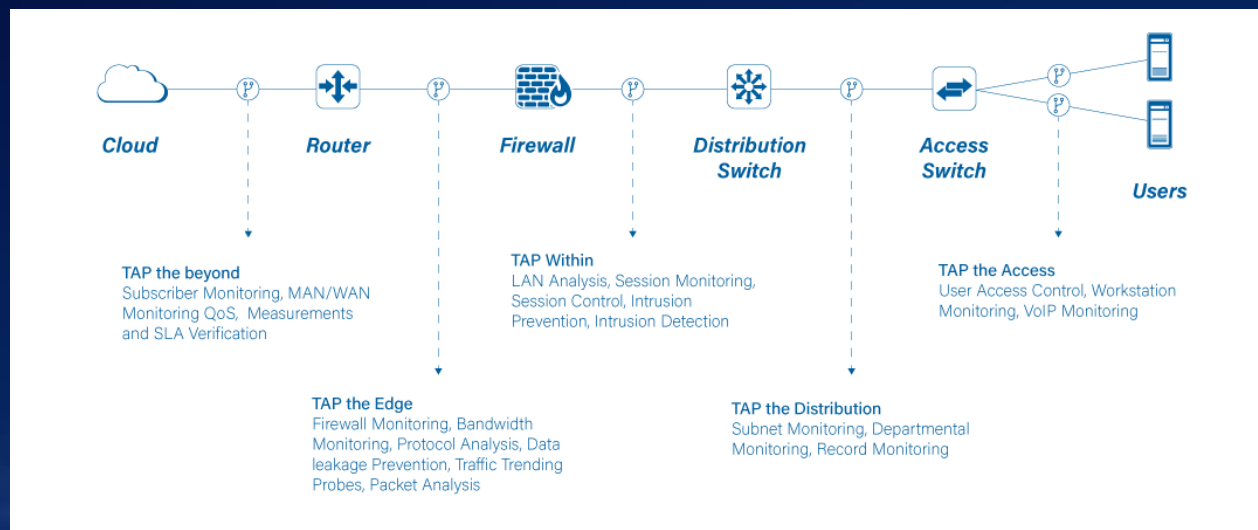
Рассмотрим:

SOFTPROM

- ✓ подходы к обеспечению наглядности сети
- ✓ как правильно снять трафик из сети без потерь
- ✓ минусы зеркалирования трафика через SPAN порт
- ✓ что такое сетевой ответвитель (TAP)
- ✓ на вкус на цвет все TAP-ы разные
- ✓ брокеры сетевых пакетов – борьба за полезный трафик
- ✓ PROFISHARK & IOTA – TAP + мониторинг из кармана

НАГЛЯДНОСТЬ СЕТИ - ПРОБЛЕМАТИКА

Задача мониторинга и контроля над сетью становится все более нетривиальной



Граница периметра теряет четкость

Точки обработки, сбора и доставки контента становятся все ближе к источнику информации.

Вызов: Больше периферийных местоположений означает больше точек сбора трафика и увеличение требований к пропускной способности сети



Миграция в облака

Распределенная сетевая инфраструктура и использование облачных сервисов приводят к тому, что вычислительные мощности, обслуживающие наши приложения, могут находиться где угодно, и менять свое физическое расположение не предсказуемо.

Вызов: Не существует простого способа физического захвата трафика при использовании облачных сервисов.

ШАГ 1 - ДОСТУП К ДАННЫМ

Как мы решаем эту задачу?



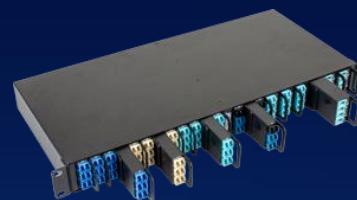
Физические точки доступа

1. Для развертывания in-line инструментов (Bypass TAP)
2. Для развертывания Out Of Band инструментов (Copper & Fiber TAPs)



Виртуальные точки доступа

1. Для публичных облаков
2. Для частных облаков



Медные и волоконные ответвители (Copper & Fiber TAPs)

- Предоставляют полную копию всех сетевых пакетов
- Безотказный и надежный доступ к сетевым данным



Bypass TAP

- Мониторинг доступности in-line инструментов (Heartbeat)
- Предотвращение простоев сети, из-за вышедших из строя in-line инструментов



Виртуальные TAP

- Централизованное управление
- Возможности по фильтрации трафика
- Простое развертывание и масштабируемость

ШАГ 2 - АГРЕГАЦИЯ И ИНТЕЛЛЕКТУАЛЬНАЯ ОБРАБОТКА ТРАФФИКА

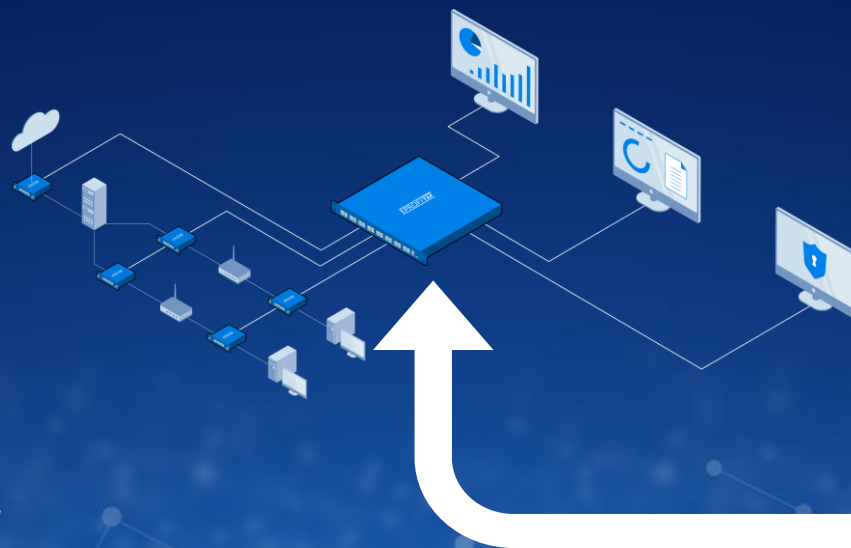
Оптимизация потока трафика между ТАР-ми и инструментами мониторинга

Важности брокеров сетевых пакетов (NPB):

- Оптимизация производительности инструментов мониторинга
- Повышение рентабельности инвестиций системы мониторинга

Линейки NPB от Profitap

- XX-Series Базовая линейка агрегаторов
- X2-Series Линейка брокеров с расширенными возможностями



Агрегация / репликация



Балансировки нагрузки



Фильтрация



Обрезка (slicing) пакетов



Временные штампы



Дедупликация пакетов



(Де) Туннелирование

ШАГ 3 - АНАЛИЗ ТРАФФИКА И ВИЗУАЛИЗАЦИЯ

Легкое устранение неполадок и сокращение среднего времени восстановления

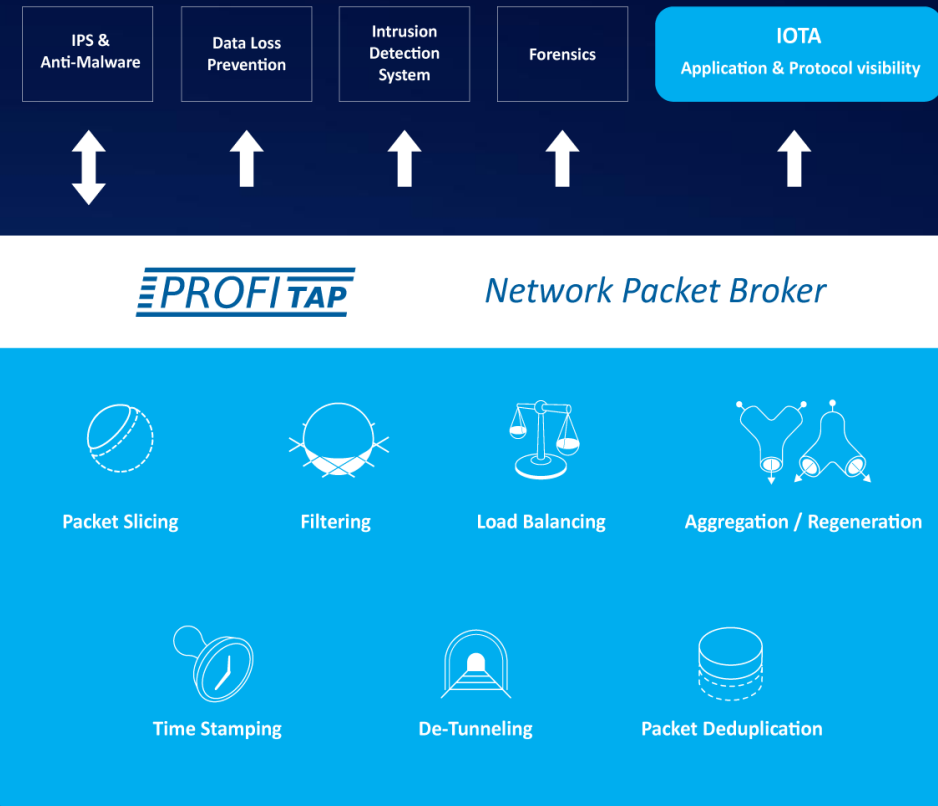
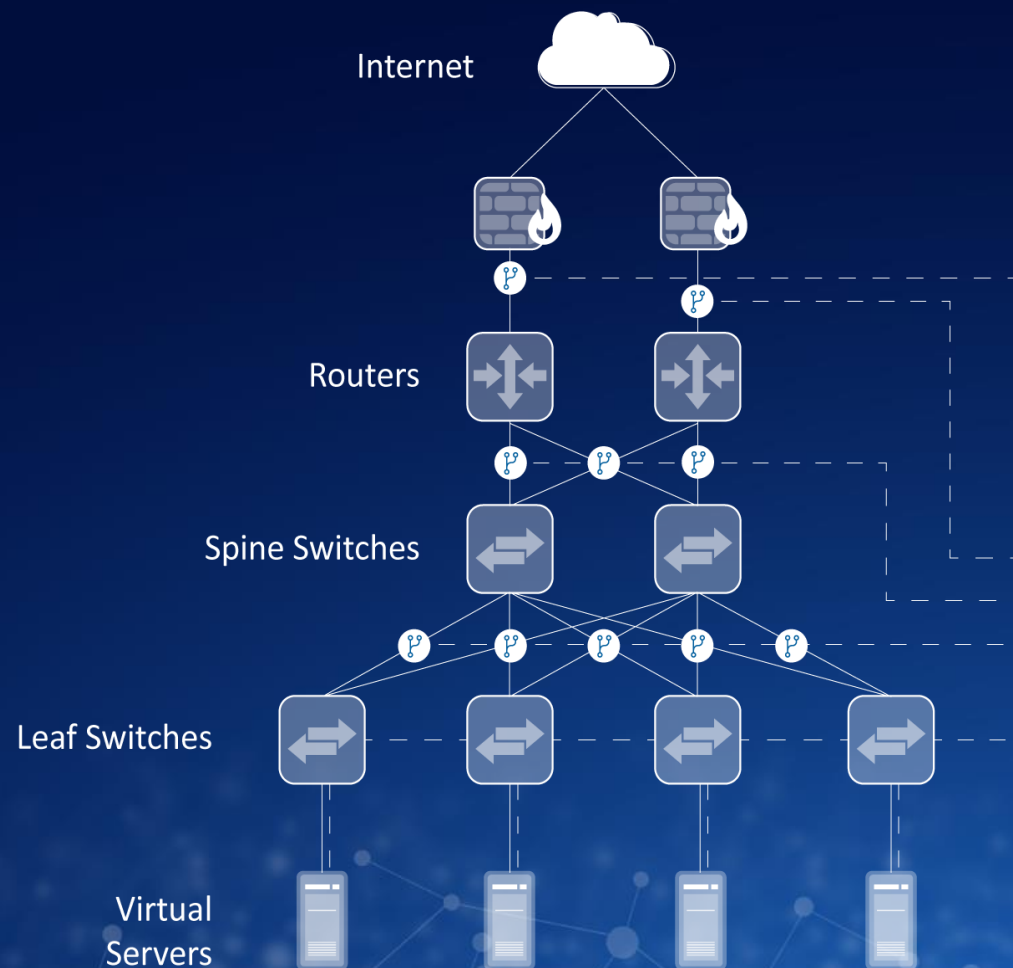
Вам нужны инструменты, которые:

- Дадут вам преимущества полного анализа пакетов и метаданных*
- Позволят проводить анализ данных как в реальном времени так и анализ сохраненных (исторических) данных*
- Максимально просты в развертывании и использовании*



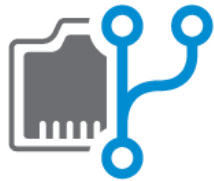
СОБЕРЕМ ВСЕ ВМЕСТЕ

SOFTPROM



PROFITAP

ПЛАТФОРМА НАГЛЯДНОСТИ СЕТИ от PROFITAP



Copper TAPs



Fiber TAPs



NPB



ProfiShark



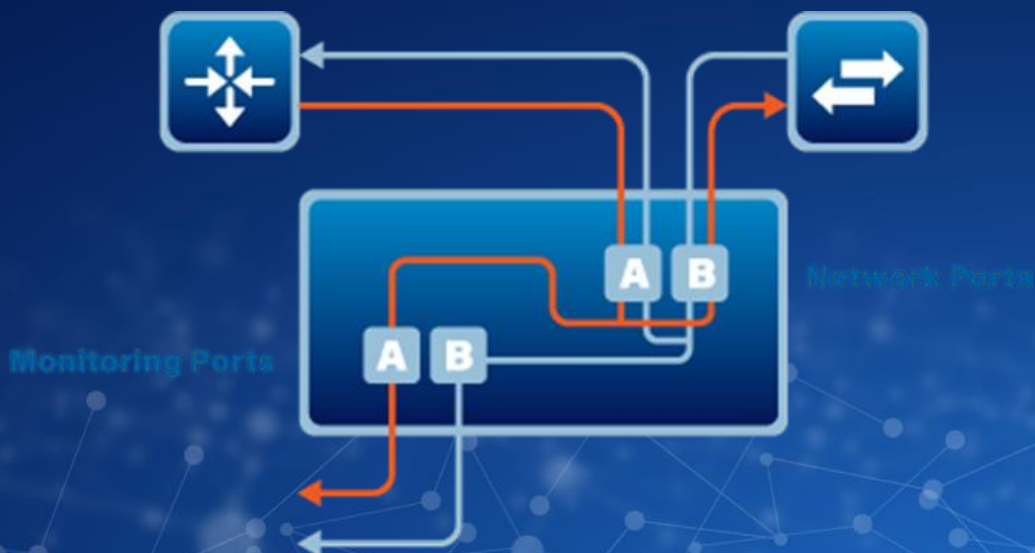
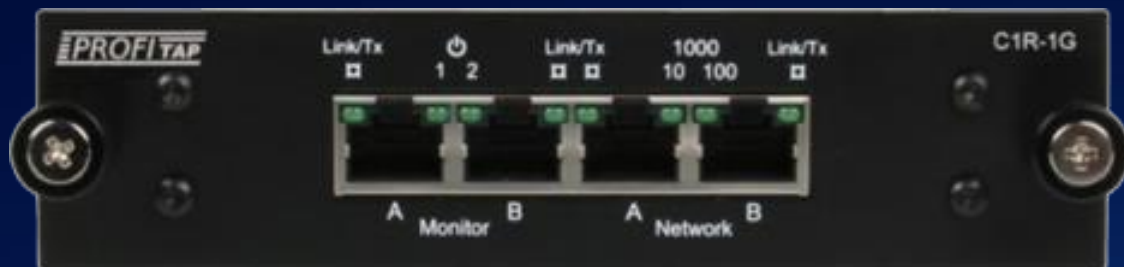
IOTA

Минусы получения трафика через SPAN (Switch Port Analyzer)

- необходимо провести настройку SPAN порта (время + стоимость администрирования)
- идет гарантированная потеря данных - Layer 1 и частично Layer 2, а также данных о поврежденных и некорректных пакетах
- есть риск потерять данные - при высокой нагрузке на коммутатор, приоритет трафика направленного на SPAN порт низкий, дроп фреймов
- мы вынуждены обрабатывать ненужные, дублирующие друг друга пакеты, их генерация обусловлена особенностями работы SPAN порта
- изменяются временные метки пакетов, что вносит ошибки в работу систем анализа трафика;
- есть риски информационной безопасности - коммутатор адресуемое сетевое устройство, соответственно SPAN порт может являться целью атаки злоумышленников
- возможность съема трафика ограничена наличием сетевого устройства и наличием доступа к нему

Сетевой ответвитель (TAP)

SOFTPROM



- не требует дополнительных настроек, единожды установленный TAP, предоставляет копию трафика на все случаи жизни

- доступ к полной копии трафика, ко всем пакетам (включая поврежденные или некорректные)

- TAP не сбрасывает пакеты при высокой нагрузке;

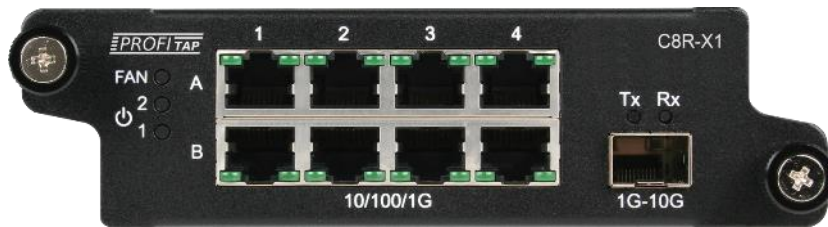
- TAP не генерирует дублирующих пакетов и не вносит изменений в копию трафика

- TAP не является адресуемым сетевым устройством, соответственно не подвержен атакам на безопасность

- TAP может использоваться как bypass решение для сторонних систем, подключаемых «в разрыв».

AGGREGATION TAPS

Aggregation of 1G to 10G



In-Line Model

Ref: C8R-X1

Aggregation of 4 x RJ45 10/100/1G in-line links into 1 x 1G-10G SFP+ output



SPAN Model

Ref: F8R-X1

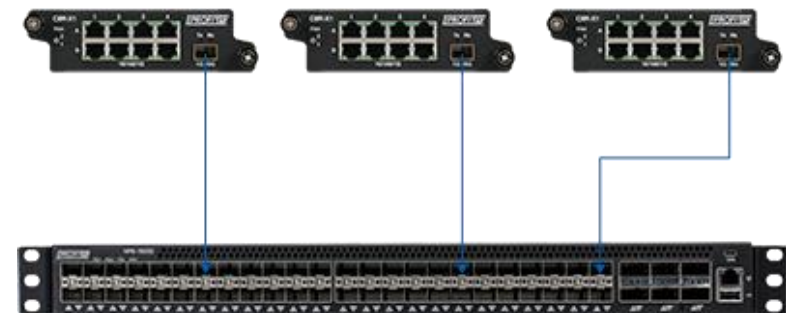
Aggregation of 8 x 1G SFP into 1G-10G SFP+ output

Features:

- Direct link aggregation, no management, installation or driver required
- VLAN Tagging
- Non-intrusive to the network
- PoE Passthrough



Portable Versions Available



REPLICATOR TAPS

Copy network traffic from one to many ports



Gigabit Replicator TAP
Ref: C1-1G-RG2

Duplicates traffic from 1 link to 2 monitoring outputs

Gigabit Port Replicator
Ref: CS1G-C4G

Duplicates all traffic from a single mirrored port onto 4 monitoring ports



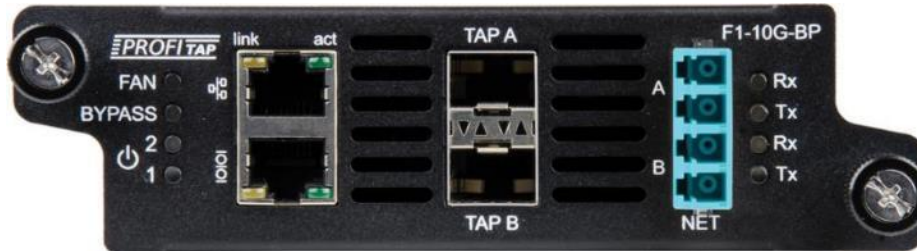
2-link LC Fiber Replicator TAP
Ref: F1L-RG2

4-link LC Fiber Replicator TAP
Ref: F1L-RG4

LC Fiber Replicator TAPs enable multiple monitoring systems to access a single LC fiber optic link. The replicator TAP only splits the signal once, before regenerate it multiple times. This greatly mitigates the weakening of the optical signal that results from excessive splitting.

BYPASS TAPS

Support active in-line network security and performance tools



10G Bypass TAP

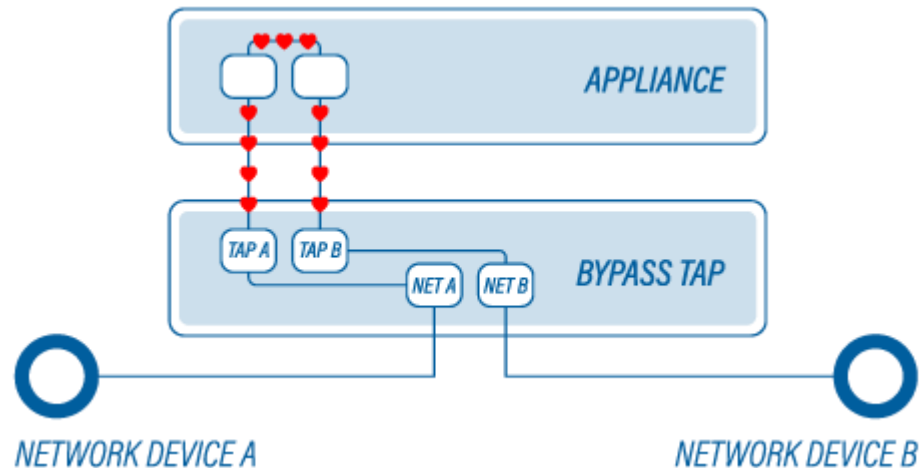
Ref: F1-10G-BP



40G Bypass TAP

Ref: F1-40G-BP

Keeping the network link operational even when in-line security appliances become unavailable.



- Protects the network link availability
- Up to 3 units in 1U rack space
- Bidirectional and configurable heartbeats
- Supports link failure propagation (LFP)
- SNMP V2c and SNMP V3 supported
- No point of failure
- Redundant powering
- Secure and completely invisible to the network
- Remote management through SSH, Web Interface (HTTPS) and SNMP Browsers

MODULAR TAPS

Up to 24 in-line TAP modules in a 1U rack space



Modular Chassis

Ref: AMC-1U

Modules available:



LC Module
Ref: F1L-MOD



MTP Module
Ref: F1M-MOD



40G BiDi Module
Ref: F1B-MOD



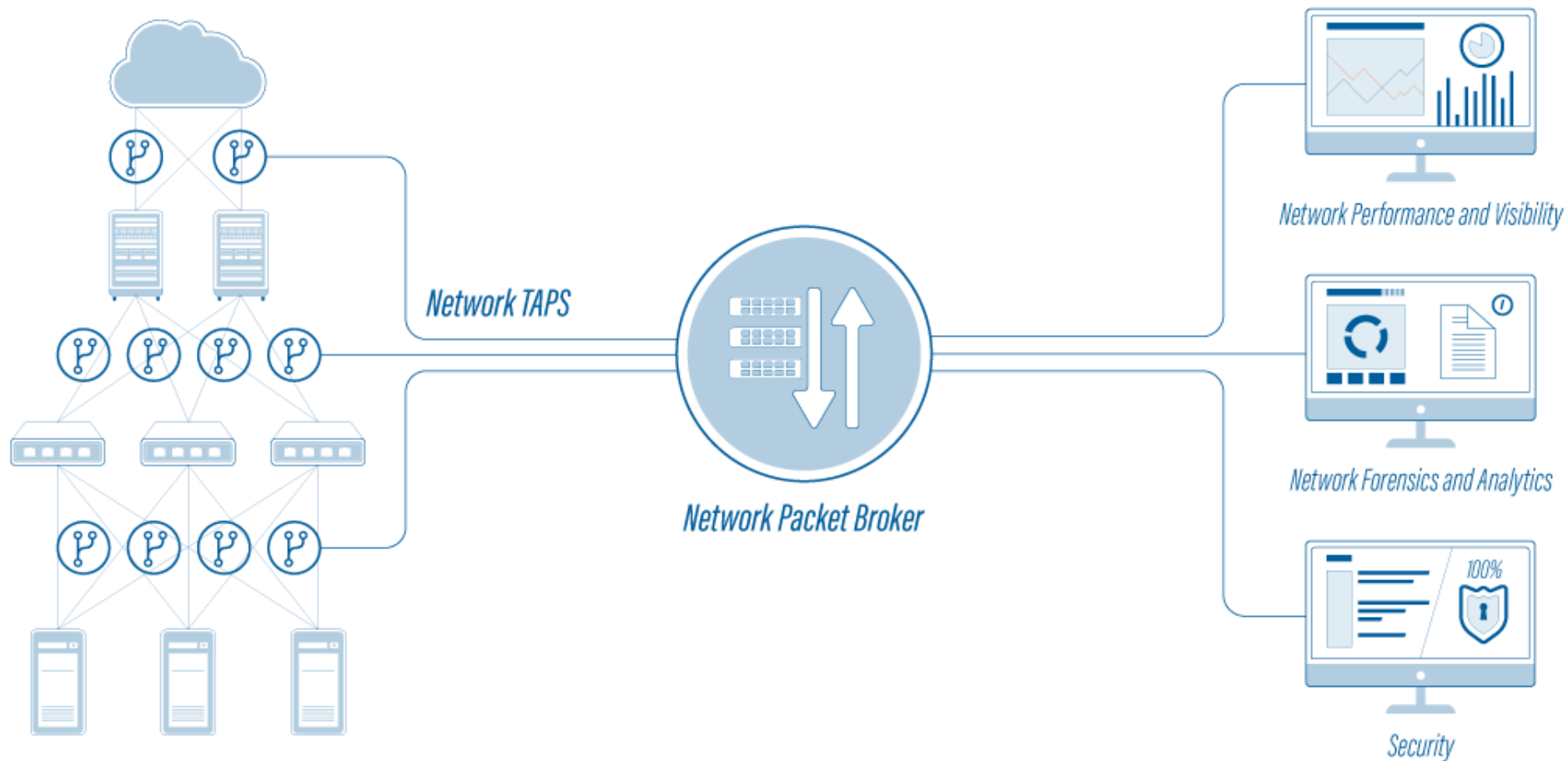
DiodeTAP Module
Ref: F1D-MOD

DiodeTAP Module:

By blocking light coming from the monitor ports, the DiodeTAP ensures total security and availability for monitored networks, while providing 100% visibility

NETWORK PACKET BROKERS

Оптимизация производительности инструментов сетевого анализа
и информационной безопасности



NETWORK PACKET BROKERS XX-Series



LOAD BALANCING

Balance traffic over multiple monitoring and security tools.



FILTERING

Only send actionable data to each of the connected tools.



AGGREGATION

Aggregate traffic coming from multiple incoming links.



REPLICATION

Replicate traffic to multiple monitoring and security tools.

XX-Series

Model	Interfaces	1Gbps	10Gbps	40Gbps	100Gbps
 XX-32G	4 x 1G SFP 2 x 10G SFP+	✓	✓	-	-
 XX-1800G	48 x 25G SFP28 6 x 100G QSFP28	✓	✓	✓	✓
 XX-2800G	48 x 25G SFP28 16x 100G QSFP28	-	✓	✓	✓
 XX-3200G	32 x 40/100G QSFP28	-	✓	✓	✓

NETWORK PACKET BROKERS X2-Series



Packet Slicing



GTP IP Filtering



Timestamping



*ERSPAN Tunneling
& De-Tunneling*



GTP Correlation



Packet Deduplication

X2-Series

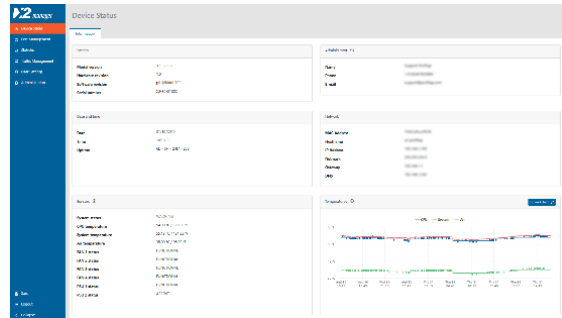
Model		Interfaces	1Gbps	10Gbps	40Gbps	100Gbps
	X2-3200G	32 x 40/100G QSFP28	-	✓	✓	✓
	X2-6400G	64 x 40/100G QSFP28	-	✓	✓	✓

- Aggregation, replication, filtering, VLAN tagging and stripping, MPLS stripping, load balancing
- Packet slicing, GTP IP filtering, GRE tunnelling & de-tunnelling, ERSPAN stripping and timestamping
- Local and remote management (CLI, GUI, SNMP, Syslog)

- Layer 2 – 4 filtering
- Flexible role-based management access
- TACACS + Authentication
- Support break-out cables

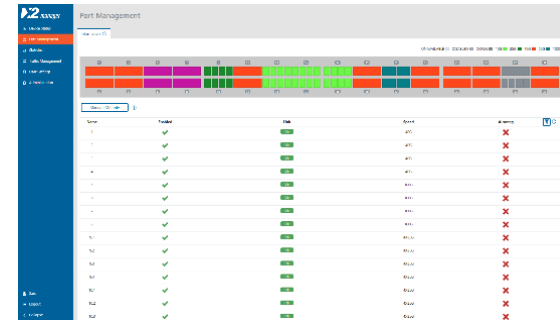
NETWORK PACKET BROKERS

XX & X2 Management applications



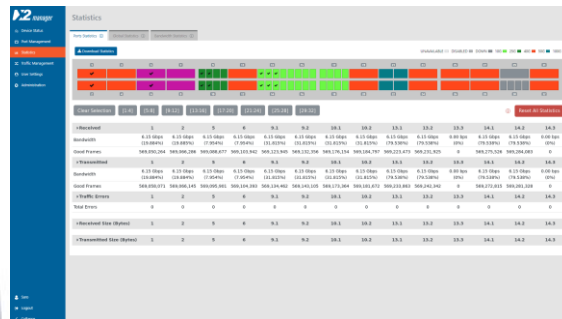
Device Status

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.



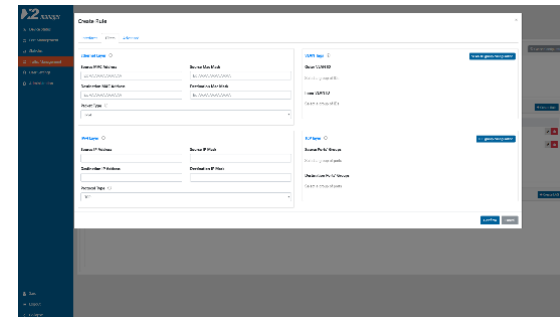
Port Management

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.



Traffic Management

Define how the traffic will flow through the device interfaces. Using a direct control interface the user will be able to define aggregation, duplication and filtering rules. Advanced actions can be defined to manipulate the traffic, adding label information or stripping undesired headers.

PROFISHARK

Portable Traffic capture



PROFISHARK

Portable Traffic capture



PROFISHARK 100M



PROFISHARK 1G



PROFISHARK 1G+



PROFISHARK 10G



PROFISHARK 10G+



- Flexibility in the field
- 100% network visibility
- Advanced timestamping capabilities
- Real-time analysis of aggregated and buffered traffic

- Hardware filtering (10G models)
- Traffic statistics
- Direct capture to disk
- Live capture

PROFISHARK MANAGER

ProfiShark Manager - 2.5.19

Counters SFP Filters Features Capture 54:10:ec:bb:00:2f

Status

ProfiShark 10G Device Connected
Driver Version : 0.1.3.50
SW Firmware Version : 0.2.3.27
HW Firmware Version : 0217
MAC Address : 54:10:ec:bb:00:2f
Usb : Super Speed

Module Present / Module Present
Software Dropped Packets : 0
Hardware Dropped Packets : 0
Link Up Duration : 0
Last Link Down Duration : 0

Firmware Update

Browse Flash Firmware

Capture Format

☐ Enable timestamps in live capture ☐ Disable Port A
☒ Transmit CRC Errors ☐ Disable Port B
☐ Keep CRC32 ☐ Packet Slicing 0 bytes

Save Restart Device

Firmware Selection

10Gbps firmware Set

ProfiShark Manager - 2.5.19

Counters Charts Log Network Ports Features Capture

Controls

Clear All
10s/division

Port A

☐ Size < 64
☐ 64 < Size < 1518
☐ Size > 1518
☐ Collisions
☐ CRC Errors
☐ Jabbers
☒ Valid Packets
☒ Invalid Packets
☒ Bandwidth Usage

Port B

☐ Size < 64
☐ 64 < Size < 1518
☐ Size > 1518
☐ Collisions
☐ CRC Errors
☐ Jabbers
☒ Valid Packets
☒ Invalid Packets

Port A

0.9
0.75
0.6
0.45
0.3
0.15
0

15:55:40 15:55:50

Port B

0.9
0.75
0.6

ProfiShark Manager - 2.5.19

Counters Charts Log Network Ports Features Capture

Status

	PortA	Port B
Link	Down	Down
Master/Slave resolution	N/A	N/A

Link Partner Status

Ports control

Any change

☐ Span Mode

Port A Configuration

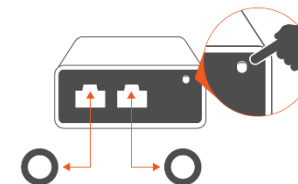
IOTA

All-In-One network analysis solution

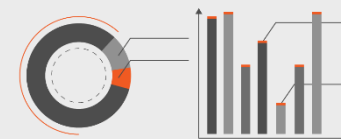
Select a line to analyze



Capture directly to disk



Visualize and analyze



IOTA

Probe - Capture - Analyze



IOTA 1G

- 10/100/1G Monitoring
- Copper
- 1TB internal storage
- Remote access

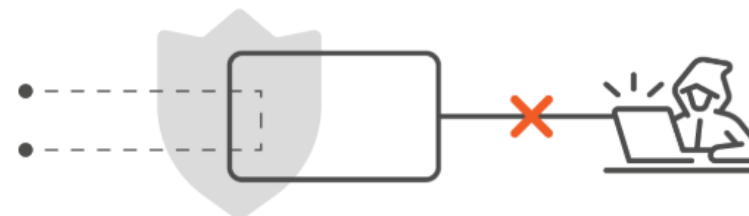


IOTA 10G

- 1G/10G Monitoring
- Copper & Fiber
- 1TB internal storage
- Remote access

Secure Deployment

IOTA's network ports are isolated from the other interfaces, internal storage and analysis processing. This makes your network safe from outside attacks while still enabling full network visibility and analysis.



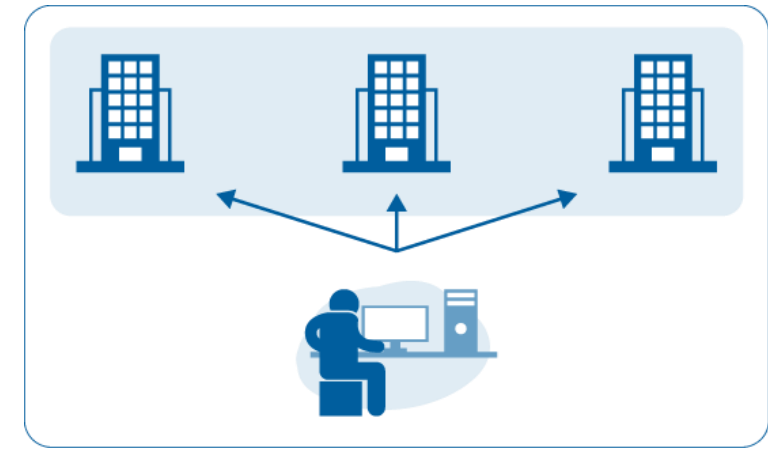
IOTA

Portable Analysis



- Ultimate network engineers portable toolkit
- Capture in person or ship IOTA for remote analysis
- Quick and easy to deploy
- Quick drill-down to network issues
- Retain raw packet capture files for DPI

Dedicated Analysis



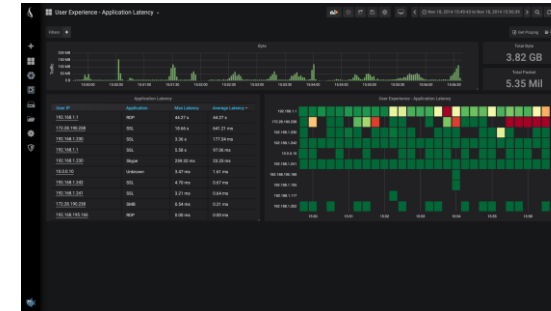
- Continuous traffic capture
- Analyze back in time
- Capture intermittent issues
- Quick insight into multiple locations
- Retain raw packet capture files for DPI

Fast drill-down with IOTA dashboards



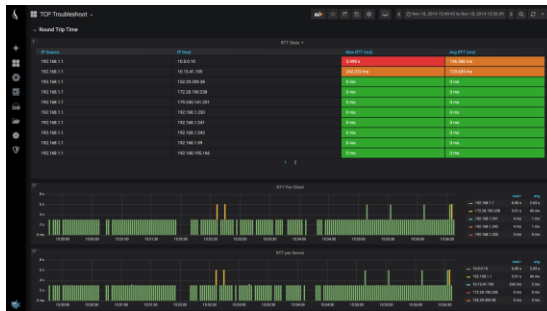
Home Dashboard

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



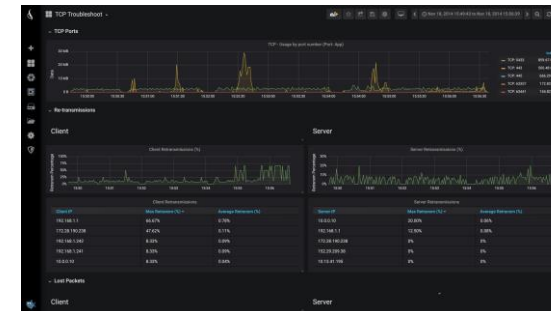
User Experience Application Latency

Application latency from the client IP perspective.



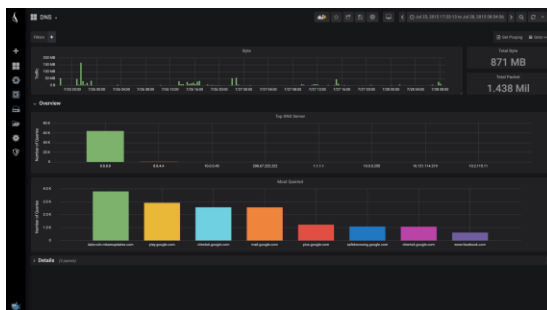
TCP Round Trip Time

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



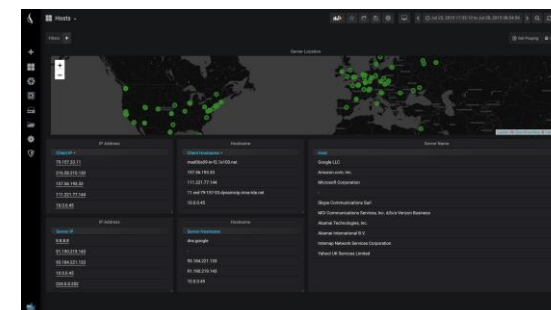
TCP Retransmissions

Retransmissions percentage over time per client and server. TCP flag statistics.



DNS Overview

Overview of top DNS servers and most queried servers.



Hosts

Overview of servers, including GeoIP resolution in map.

ПОЧЕМУ PROFITAP

Инженерная направленность: Разрабатывает и производит продукцию собственными силами

Опыт: Более 37 лет опыта в отрасли

Качество: Фокус на высокой производительности и долговечности

Надежность: Строгий контроль качества продукции

Оперативность: Кратчайшие сроки выполнения заказа

Инновационный подход: Уникальный ассортимент продукции

Гибкие исследования и разработки: производит специализированные продукты по спецификации клиента

Служба поддержки: Именно там, где нужны и когда нужны



Высокое качество

Продукция тестируется до и после сборки, чтобы гарантировать высочайшие стандарты качества.



Инновации

Мы производим и поставляем инновационные решения для мониторинга исключительно собственной разработки



Глобальное покрытие

Наши продукты стали комплексным решением для более чем 1000 клиентов из 60 стран мира.



С нами легко работать

Мы предлагаем бесплатный доступ к службе технической поддержки как к единой точке контакта.

PROFITAP

SOFTPROM

Александр Кобец
Менеджер по развитию бизнеса
+38 (096) 798-78-02
kobets@softprom.com

