

АКМЕТРОН

KEYSIGHT · NETWORK VISIBILITY



СЕТЕВЫЕ ТАР

NETWORK TAPS

Практическое руководство по проектированию, выбору, испытаниям и эксплуатации

Актуализация: август 2026

НАЗНАЧЕНИЕ ДОКУМЕНТА

Руководство для инженеров и лиц, принимающих решения

Как выбрать точки наблюдения, рассчитать оптический и пакетный тракт, сравнить TAP со SPAN и облачным зеркалированием, доказать характеристики в PoC и безопасно эксплуатировать инфраструктуру доступа к трафику.

КЛЮЧЕВОЙ ПРИНЦИП

TAP является источником копии трафика, но не гарантией результата. Полнота и достоверность видимости ограничиваются всей цепочкой: точка установки → TAP → физический monitor-path → NPВ или capture NIC → инструмент.

Для кого предназначено руководство

Роль	Какие решения помогает принять документ
Сетевой архитектор	Где устанавливать TAP, как выбрать тип, скорость, оптику, split ratio и схему доставки.
Инженер ЦОД / СКС	Как проверить тип волокна, полярность, оптический бюджет, маркировку и монтаж.
SOC / SecOps	Как получить достоверный feed для NDR, IDS, PCAP и форензики без скрытых потерь.
NOC / NetOps	Как отделять производственные ошибки от потерь monitor-path и эксплуатировать точки доступа.
ЛПР / закупки	Как формировать RFP, сравнивать TAP, считать TCO и принимать решение по измеримому PoC.

Как использовать документ

Определить цель наблюдения, критические сервисы и требуемую доказательность пакетов.
Выбрать физические или виртуальные точки доступа и выполнить расчеты live-path и monitor-path.
Перенести обязательные требования в RFP и связать каждое требование с методом проверки.
Провести лабораторные и приемочные испытания, включая потерю питания и пиковую двунаправленную нагрузку.
Передать эксплуатации схемы, baseline измерений, thresholds, runbook и ответственных владельцев.

ОГРАНИЧЕНИЕ

Руководство не заменяет datasheet, release notes, compatibility matrix и проектную документацию. Численные характеристики подтверждаются для конкретной модели, аппаратной ревизии и схемы подключения.

Содержание

Раздел	Практический результат
01. Резюме и границы применения	Понимание ценности, рисков и критериев решения.
02. Архитектура и терминология	Корректная модель live-path и monitor-path.
03. Типы TAP и режимы работы	Выбор passive/active, breakout/aggregation/regeneration.
04. Оптическое проектирование	Расчет четырех трактов, split ratio, PMD, FEC и приемка.
05. Медные TAP	PoE, auto-negotiation, fail-to-wire и тесты отказа.
06. TAP, SPAN, cloud mirror и bypass	Выбор подходящего метода получения трафика.
07. Архитектуры развертывания	Точки наблюдения для ЦОД, филиала, ОТ и hybrid cloud.
08. Безопасность и шифрование	Изоляция monitor-портов, TLS/QUIC и governance данных.
09. Выбор решения и RFP	Нейтральная матрица требований и актуальные примеры.
10. PoC и приемка	Единая программа испытаний и измеримые критерии PASS/FAIL.
11. Эксплуатация и экономика	Runbook, диагностика, RACI, TCO и инвестиционное решение.
Приложения А–Е	Заполняемые формы, чек-листы, глоссарий и источники.

Навигация по ролям

Роль	Приоритетные разделы
Сетевой архитектор	02–07, 09–10
Инженер ЦОД / СКС	03–05, 10, приложение С
SOC / SecOps	01, 06–08, 10–11
ЛПР / закупки	01, 09, 11, приложение А
Эксплуатация	05, 07, 10–11, приложения В–С

01

РЕЗЮМЕ И ГРАНИЦЫ ПРИМЕНЕНИЯ

Почему TAP нужен, где он оправдан и что именно необходимо доказать

Решение для ЛПР

Сетевой TAP следует рассматривать как элемент инфраструктуры наблюдаемости, а не как аксессуар анализатора. Его ценность возникает там, где пропущенный пакет, временная конфигурация SPAN или невозможность воспроизвести инцидент создают неприемлемый операционный или киберриск.

Если требуется	Предпочтительный подход	Причина
Постоянный доступ к критичной физической линии	Аппаратный TAP	Независимость от конфигурации коммутатора и выделенный monitor-path.
Краткая диагностика порта или VLAN	SPAN	Быстро, без разрыва линии и дополнительных устройств.
Удаленная копия через IP-сеть	ERSPAN / tunnel mirror	Не нужен локальный анализатор, но появляются MTU и transport risks.
Видимость VM или cloud workload	vSwitch/vTAP/cloud mirror	Физический TAP не видит трафик, не покидающий host или cloud fabric.
Подключение inline IPS/NGFW	Bypass switch	Нужны fail-open/fail-close и контролируемое исключение инструмента из live-path.

ПОЛНОТА ВИДИМОСТИ ОПРЕДЕЛЯЕТСЯ ВСЕЙ ЦЕПОЧКОЙ



Рисунок 1. Гарантировать необходимо не TAP отдельно, а сквозной тракт доставки пакетов.

Когда TAP особенно оправдан

- инциденты ИБ и форензика требуют воспроизводимой полной последовательности пакетов;
- критическая линия работает близко к загрузке, при которой SPAN destination может быть перегружен;
- необходимо наблюдать оба направления независимо и сохранять исходный порядок;
- изменение или перезагрузка коммутатора не должны отключать мониторинг;
- несколько инструментов должны получать один и тот же трафик через NPB или regeneration;
- ошибка точки наблюдения имеет большую стоимость, чем контролируемое окно установки TAP.

Что TAP не решает

Ограничение	Что требуется дополнительно
Не анализирует пакеты	NDR/IDS, packet recorder, NPM/APM или protocol analyzer.

Ограничение	Что требуется дополнительно
Не расшифровывает TLS, QUIC, IPsec или MACsec	Endpoint/proxy telemetry, контролируемая дешифрация или анализ метаданных.
Не гарантирует отсутствие drops downstream	Расчет емкости, counters, NPB, capture NIC и контроль storage.
Не создает timestamp автоматически	Capture NIC/NPB/analyzer и синхронизация PTP/NTP.
Не заменяет измерение физического уровня	DOM/DDM, power meter, FEC/CRC counters, BERT при необходимости.

КРИТЕРИЙ УСПЕХА

Проект считается успешным, если нужный пакет в нужном направлении поступает в нужный инструмент с измеренной полнотой, корректным временем и известной политикой обработки — включая аварийные режимы.

Контрольные вопросы до начала проекта

Вопрос	Что должно быть зафиксировано
Какой сервис защищаем?	Владелец, критичность, SLA и допустимое окно работ.
Какое событие доказываем?	Нужные пакеты, направления, ошибки, timestamp и срок хранения.
Где находится нужный контекст?	До/после NAT, firewall, proxy, TLS termination и load balancer.
Какова пиковая нагрузка?	Гбит/с, Mpps, duplex, IMIX, jumbo и microbursts.
Кто отвечает за результат?	Владельцы live-path, TAP, NPB, tools, данных и изменений.
Как принимаем решение?	Численные PASS/FAIL, evidence и порядок обработки отклонений.

02

АРХИТЕКТУРА И ТЕРМИНОЛОГИЯ

Network A/B, monitor A/B, live-path, monitor-path и границы ответственности

РАБОЧИЙ ТРАКТ И ТРАКТ МОНИТОРИНГА

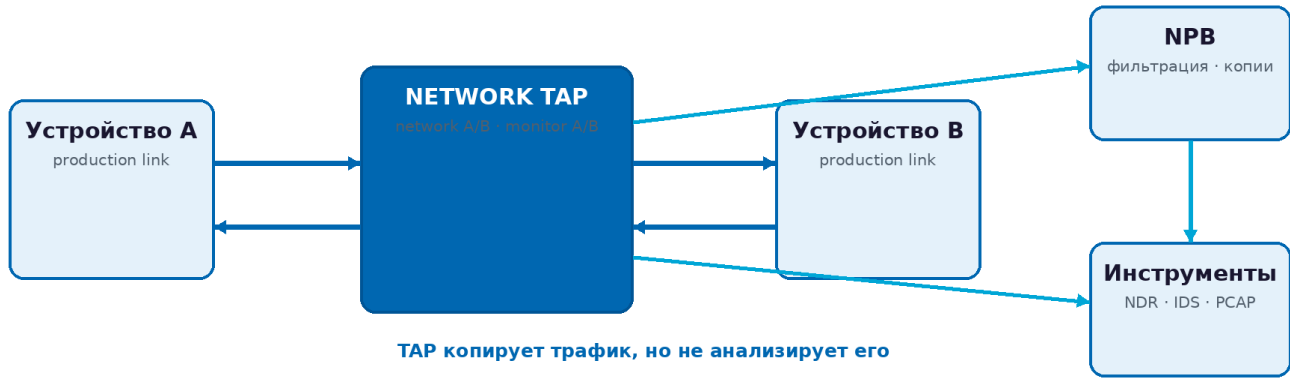


Рисунок 2. Базовая архитектура аппаратного ТАП и последующей доставки трафика.

Определение

Network TAP — специализированная точка получения копии трафика, устанавливаемая в физический канал или реализуемая как функция активного устройства. В отраслевых материалах встречаются расшифровки Test Access Port, Test Access Point и Traffic Access Point. В этом руководстве используется термин «сетевой ТАП» без привязки к единственной расшифровке.

Термин	Определение	Что контролировать
Network ports A/B	Порты рабочего соединения	Скорость, среда, PMD, continuity и поведение при отказе.
Monitor A/B	Копии соответствующих направлений	Rx-only/air gap, мощность, скорость и формат кадров.
Live-path	Рабочий путь между узлами	Доступность, insertion loss, latency и link events.
Monitor-path	Путь от ТАП до инструмента	Drops, MTU, oversubscription, timestamp и tool capacity.
Observation point	Место, где снимается трафик	NAT, encryption, routing, load balancing и visibility scope.

Что происходит с полнодуплексным трафиком

- пакеты A→B и B→A передаются по live-path;
- breakout-ТАП выводит два направления на отдельные monitor-порты;
- агрегирующий ТАП может объединять направления в один egress, если хватает емкости;
- регенерация формирует несколько копий для нескольких инструментов;
- конечный анализатор должен знать, как определить направление и не перепутать копии.

Корректные формулировки требований

Недостаточная формулировка	Инженерная формулировка
ТАП дает 100% трафика	0 необъясненных потерь во всей monitor-chain при заданном профиле, нагрузке и длительности.

Недостаточная формулировка	Инженерная формулировка
Передаёт все ошибки	Перечень типов кадров/ошибок, которые подтверждены TAP, приемником и инструментом.
Не влияет на сеть	Измерены insertion loss, link events, latency и режимы питания для выбранной модели.
Безопасный monitor-порт	Подтверждено физическое блокирование обратной передачи для конкретного устройства.
Мгновенное восстановление	Измерено время переключения и число потерянных/дублированных пакетов.

ВРЕМЕННЫЕ МЕТКИ

Пассивный TAP обычно не добавляет timestamp. В проекте фиксируются точка timestamping, источник времени, допустимая погрешность, holdover и совместимость формата с анализатором.

Паспорт направлений A/B

Поток	Network input	Monitor output	Получатель / проверка
A→B	Network A	Monitor A	Rx A инструмента; маркированный test flow
B→A	Network B	Monitor B	Rx B инструмента; маркированный test flow
Aggregated	A→B + B→A	Monitor aggregate	Метаданные направления, capacity и drops

Сквозная цепочка приемки

- ☐ Счетчики источника и приемника production-линии сохранены как baseline.
- ☐ Network и monitor-порты TAP однозначно промаркированы.
- ☐ NPB/capture NIC не показывают drops, overruns или congestion без объяснения.
- ☐ Инструмент получил ожидаемое число последовательных пакетов каждого направления.
- ☐ Место timestamping и состояние источника времени внесены в отчет.

03

ТИПЫ TAP И РЕЖИМЫ РАБОТЫ

Пассивные и активные конструкции, breakout, aggregation, regeneration и защищенные исполнения

РЕЖИМЫ ДОСТАВКИ КОПИЙ

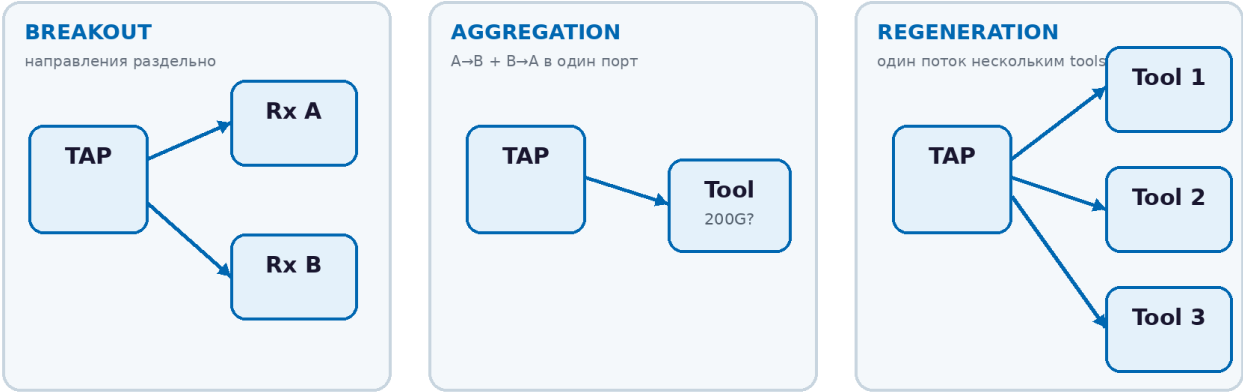


Рисунок 3. Breakout сохраняет направления, aggregation экономит порт, regeneration масштабирует число потребителей.

Классификация по среде и конструкции

Класс	Преимущества	Ограничения / проверки
Пассивный оптический	Нет питания в live-path, нет IP-адреса, минимальная логика отказа.	Оптический бюджет, split ratio, тип волокна/PMD, поляриность и monitor receiver.
Активный оптический	Возможны преобразование, aggregation, regeneration и управление.	Питание, latency, behavior при отказе и feature capacity.
Активный медный	Поддержка BASE-T, auto-negotiation, возможны PoE и fail-to-wire.	Согласование линка, PoE class, питание A/B и время восстановления.
Patch TAP	Интеграция в патч-панель, низкая плотность кабелей и постоянная точка доступа.	Совместимость модулей, cross-connects, маркировка и insertion loss.
Tough/industrial	Расширенный температурный диапазон и монтаж для ОТ/удаленных площадок.	Сертификация среды, вибрация, DIN/rack, питание и сервисный доступ.
Secure TAP	Дополнительная защита monitor-path и портов.	Механизм защиты, световая инъекция, доступ к кассетам и модель угроз.

Breakout

Два направления выводятся отдельно. Это наиболее предсказуемый режим для forensic capture: емкость каждого monitor-порта равна скорости одного направления, а инструмент или NPB получает явную информацию о направлении.

Aggregation

РАСЧЕТ

Для линии 100G full duplex теоретический суммарный поток может достигать 200 Гбит/с. Один выход 100G не способен гарантированно передать оба направления при одновременной полной нагрузке.

Параметр	Что зафиксировать
Входная нагрузка	Peak A→B + peak B→A, Mpps, packet-size distribution и microbursts.
Egress capacity	Фактическая скорость monitor-порта и ограничение внутренней коммутации.
Очереди	Buffer, arbitration, drops counters, watermarks и alarm thresholds.
Direction metadata	Как downstream-инструмент различает направления после агрегации.
Failure behavior	Что происходит при недоступности или снижении скорости tool-порта.

Regeneration и TAP→NPB

Регенерация полезна, когда одинаковый raw feed нужен нескольким независимым средствам. Для масштабной фильтрации, балансировки, преобразования скоростей и контроля нескольких источников предпочтительна связка TAP→NPB→tools.

Задача	Regeneration	NPB
Несколько идентичных копий	Да	Да
Фильтрация по заголовкам	Обычно нет	Да, зависит от модели
Балансировка пула tools	Нет	Да
Переход скоростей	Ограниченно	Да, в пределах port/capacity
Централизованные counters и policy	Ограниченно	Да

Расчет monitor-capacity

Сценарий	Минимальная емкость	Что проверить
10G breakout	2 × 10G Rx	Каждое направление и оба capture rings.
100G aggregation	До 200 Гбит/с суммарно	Oversubscription, buffers, drops и направление.
100G regeneration ×3	3 независимых 100G egress	Внутренняя fabric capacity и tool outages.
400G→4×100G через NPB	400G ingress + 4×100G egress	Mpps, hash, packet affinity и headroom.

ПЛАНИРОВАНИЕ

Средняя загрузка недостаточна для оценки. Используйте одновременный peak обоих направлений, максимальный Mpps и microburst profile; резерв мощности фиксируйте как проектное требование.

04 ОПТИЧЕСКОЕ ПРОЕКТИРОВАНИЕ

Бюджет мощности, split ratio, типы волокна, lane architecture, PAM4 и FEC

ОПТИЧЕСКИЙ БЮДЖЕТ: ЧЕТЫРЕ ТРАКТА

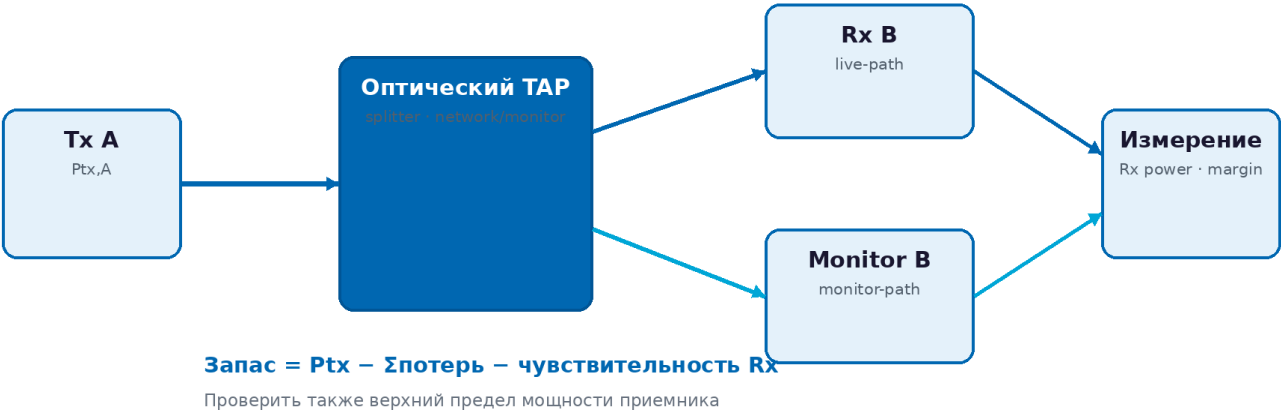


Рисунок 4. Оптический бюджет рассчитывается отдельно для live-path и monitor-path в обоих направлениях.

Расчет оптического бюджета

ОСНОВНАЯ ФОРМУЛА

Запас, дБ = минимальная Tx power – суммарные потери тракта – минимальная чувствительность Rx.
Результат должен оставаться положительным с согласованным эксплуатационным запасом [2].

Слагаемое потерь	Что включить	Evidence
Волокно	Длина × затухание на рабочей длине волны	Проект СКС / измерение
Коннекторы	Каждая разъемная пара, включая patch panels	Норматив/измерение
Сварки	Все постоянные соединения	Рефлектограмма / паспорт
ТАР	Network insertion loss и monitor insertion loss	Datasheet конкретной модели
Прочие элементы	Mux/Demux, адаптеры, кассеты, cross-connects	Datasheet / измерение
Запас	Загрязнение, старение, температура, ремонт и перекоммутация	Политика проекта

Четыре обязательных расчета

Тракт	Приемник	Проверка
A→B live	Rx B	После network leg ТАР мощность выше чувствительности и ниже overload.
B→A live	Rx A	Отдельный Tx budget второго направления.
A→monitor	Monitor Rx A	Monitor leg, длина patch, приемник analyzer/NPB.
B→monitor	Monitor Rx B	Независимый расчет и измерение.

Split ratio

Коэффициент указывается как network/monitor. Большая доля в live-path уменьшает влияние на рабочую сеть, но требует более чувствительного monitor receiver. Теоретическое деление дополняется excess loss и потерями соединителей [3].

Split network/monitor	Пример insertion loss SM network/monitor	Инженерный смысл
50/50	3,7 / 3,7 дБ	Симметричный бюджет; обе стороны требуют заметного запаса.
60/40	2,8 / 4,8 дБ	Приоритет live-path при умеренном ослаблении monitor.
70/30	2,0 / 6,1 дБ	Типовой компромисс, если analyzer имеет достаточную чувствительность.
80/20	1,3 / 8,0 дБ	Малое влияние на live, жесткий monitor budget.
90/10	0,8 / 12,0 дБ	Максимальный приоритет live; monitor может потребовать short reach/чувствительную оптику.

Значения выше приведены как пример из таблицы Ixia Flex Taps [4] и не являются универсальными. Для нового проекта используются актуальные параметры выбранной модели и оптики.

Физическая совместимость

Параметр	Варианты	Риск ошибки
Волокно	OS2, OM3, OM4, OM5	Несовместимые modal bandwidth, wavelength и reach.
Коннектор	LC duplex, MPO/MTP	Неверная polarity, key orientation или число волокон.
PMD	SR4/SR8, DR4/DR8, FR4, LR4, PSM4	Одинаковая скорость, но разная lane/wavelength architecture.
BiDi	Две длины волны на одном волокне	Обычный duplex TAP неприменим; нужен специализированный BiDi.
WDM	CWDM/DWDM или LAN-WDM	Splitters и мониторные приемники должны соответствовать спектру.
Transceiver	Tx min/max, Rx sensitivity/overload, DOM	Link может подняться без достаточного эксплуатационного запаса.

100/200/400G и планирование 800G/1.6T

IEEE 802.3df-2024 добавляет параметры для 800 Gb/s и 1.6 Tb/s [1]. Однако скорость на этикетке не описывает число lanes, PMD, FEC и разъем. На дату актуализации портфель Keysight TAP заявляет поддержку до 400G [9]; поддержку более высоких скоростей следует подтверждать дорожной картой и PoC.

Область	Проверить
PAM4 / lane rate	Соответствие PMD и monitor receiver, а не только aggregate Ethernet rate.
FEC	Режим, corrected/uncorrectable counters, состояние до и после установки TAP.
MPO/MTP	Polarity, lane order, число волокон, clean/inspect before connect.
Breakout	Допустимые fan-out комбинации и соответствие analyzer/NPB.
Roadmap	Конкретные part numbers, сроки, совместимость и upgrade path.

Приемка оптической линии

- ☐ Сохранены Tx/Rx power и DOM до установки ТАР.
- ☐ Рассчитаны и измерены оба live-path и оба monitor-path.
- ☐ Проверен overload threshold каждого приемника.
- ☐ Коннекторы очищены и осмотрены; polarity и маркировка соответствуют схеме.
- ☐ Сравнены CRC, PCS/FEC corrected и uncorrectable counters до и после установки.
- ☐ Подтверждена стабильность линка под трафиком и после перекоммутации.

Рабочая форма оптического бюджета

Тракт	Tx min, dBm	Σ потерь, dB	Rx / запас / вывод
A→B live	_____	_____	_____ / _____ / _____
B→A live	_____	_____	_____ / _____ / _____
A→monitor	_____	_____	_____ / _____ / _____
B→monitor	_____	_____	_____ / _____ / _____

Монтажная последовательность

Проверить BOM, PMD, длину волны, connector, polarity и рабочее окно.
Сохранить baseline Tx/Rx, DOM, FEC/CRC и link events до разрыва линии.
Очистить и осмотреть коннекторы, установить ТАР по схеме A/B.
Сначала подтвердить оба live-path, затем подключить monitor receivers.
Выполнить power, packet и failure tests; записать серийные номера и фактические значения.

05

МЕДНЫЕ ТАР

Auto-negotiation, PoE, fail-to-wire, питание и проверка рабочего канала

Почему медный ТАР является активным устройством

Для BASE-T требуется согласование и восстановление электрического сигнала, поэтому медный ТАР обычно нуждается в питании для monitor-функции. Наличие fail-to-wire должно подтверждаться конструкцией и испытанием: оно не означает отсутствие link flap, renegotiation или потери активных сессий.

Параметр	Требование проекта	Испытание
Скорость	10/100/1000 и при необходимости 2.5/5/10GBASE-T	Каждая требуемая скорость и duplex.
Auto-negotiation	Совместимость обоих endpoints	Power cycle и повторное согласование.
PoE	Тип, класс, пары, мощность и направление	Нагрузка PoE и снятие питания ТАР.
Jumbo frames	Максимальный размер кадра	Line rate без изменения/усечения.
EEE	Поддержка или документированный запрет	Переходы idle/active и latency.
Fail-to-wire	Live continuity при потере обоих PSU	Измерить gap, renegotiation и восстановление.
Monitor isolation	Rx-only/data diode при необходимости	Попытка передачи обратно в live-path.

Матрица отказов

Событие	Что измерить	Недостаточный результат
Отказ PSU A	Alarm и непрерывность monitor/live	Скрытое отключение копий.
Отказ PSU B	Аналогично для резервного ввода	Резерв не проверен.
Отказ обоих PSU	Packet gap, link state, PoE continuity	Fail-to-wire заявлен без численного подтверждения.
Восстановление питания	Повторный gap и monitor recovery	Live-path перезапускается вторично.
Отключение tool	Отсутствие влияния на live	Tool-порт способен воздействовать на сеть.
Замена кабеля	Speed/duplex/PoE и counters	Непредсказуемое согласование.

ПРИМЕР МОДЕЛИ

Keysight IxTap Copper заявляет 10/100/1000, redundant power, fail-to-wire, PoE и jumbo pass-through, а также air-gapped monitor ports [11]. Эти свойства относятся к данной модели и должны проверяться для выбранной ревизии.

Минимальный протокол медной приемки

- Записать speed/duplex, PoE class и counters endpoints до установки.
- Проверить line-rate для минимальных кадров, IMIX и jumbo frames в обоих направлениях.
- Поочередно отключить источники питания ТАР, затем оба источника.
- Измерить link flap, packet loss, время восстановления и состояние PoE.
- Попытаться передать тестовый кадр через monitor-порт обратно в live-сеть, если заявлен data diode.
- Сохранить итоговые counters, конфигурацию и serial/firmware в акте приемки.

06 TAP, SPAN, CLOUD MIRROR И BYPASS

Платформозависимые ограничения, выбор метода и доказуемость полученной копии

КАК ВЫБРАТЬ ИСТОЧНИК КОПИИ ТРАФИКА

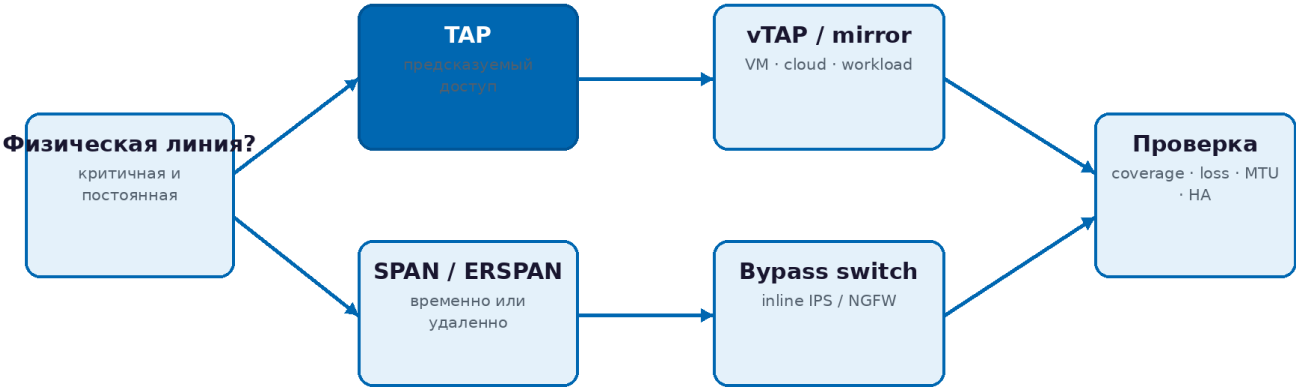


Рисунок 5. Выбор метода определяется средой, критичностью и ролью инструмента.

Сравнение методов

Критерий	TAP	SPAN/ERSPAN	vTAP/cloud mirror	Bypass
Основная роль	Постоянная копия физической линии	Зеркалирование switch/router	Копия виртуального workload	Подключение inline tool
Зависимость от config	Минимальная/модельная	Высокая	Policy/API/tags	Fail policy и health
Перегрузка	В downstream или aggregation	В destination/fabric/tunnel	В source/target/transport	В inline tool
FCS/errors	Зависит от TAP и receiver	Платформозависимо	Обычно уже обработанные packets	Не основная задача
Удаленный доступ	Через NPB/tunnel	ERSPAN	Нативно	Через management/NPB
Разрыв линии при монтаже	Да	Нет	Нет физического разрыва	Да

SPAN: что можно утверждать корректно

SPAN удобен и часто достаточен для временной диагностики, но его поведение определяется платформой, ASIC, версией ОС и конкретной сессией. Нельзя переносить ограничения одного коммутатора на все устройства.

Подтвержденный пример	Практическое следствие
Cisco Catalyst указывает, что oversubscribed SPAN destination может терять пакеты [5].	Рассчитывать суммарный Rx+Tx peak и проверять destination drops.
Catalyst описывает возможную отправку двух копий одного пакета при сочетании Rx и Tx sources [5].	Проверять duplicates и топологию source interfaces.
Cisco Nexus 9000 указывает, что пакеты с FCS errors не зеркалируются [6].	Для физической диагностики конкретной платформы SPAN может быть недостаточен.
Точка репликации относительно ACL/QoS влияет на содержимое копии [5][6].	Документировать ingress/egress и ожидаемую стадию обработки.

Cloud mirroring

Риск	Что включить в проект
Encapsulation overhead	Размер заголовков, source/target MTU и допустимое усечение.
Transport loss	Пропускная способность ENI/vNIC, target, tunnel и collector.
Coverage drift	Автоматическое включение новых workloads по tag/policy и контроль исключений.
Стоимость	Compute, inter-AZ/region traffic, egress и хранение.
Failure domain	Instance/AZ/region failure, autoscaling и health checks.

AWS MTU

AWS документирует дополнительный overhead Traffic Mirroring и возможность truncation при недостаточном target MTU [7]. Проверка должна выполняться на максимальном размере исходного пакета.

TAP и bypass switch

Характеристика	TAP	Bypass switch
Инструмент	Out-of-band NDR/IDS/PCAP/NPM	Inline IPS/NGFW/DLP
Live traffic через инструмент	Нет	Да или через bypass path
Основной отказ	Потеря копии / влияние вставки	Потеря/блокировка production traffic
Ключевая политика	Breakout/aggregation/regeneration	Fail-open/fail-close и heartbeat
Приемка	Completeness и monitor-chain	Session continuity и switch time

Когда SPAN достаточен

разовая диагностика на линии с низкой критичностью и известным запасом destination-порта;
лабораторная среда, где допустима повторная конфигурация и потеря части evidence;
контроль ограниченного набора VLAN/портов при документированных platform limits;
временный источник до установки постоянной точки наблюдения, с назначенным сроком отключения.

Контрольная карточка зеркалирования

Поле	Зафиксировать
Source / direction	Порты, VLAN, Rx/Tx/both и стадия обработки.
Destination / transport	Порт, tunnel, target, collector и маршрут.
Нагрузка	Peak Гбит/с, Mpps, duplicates и oversubscription.
MTU	Исходный max frame, encapsulation overhead и truncation policy.
Контроль	Drops, queues, health, coverage drift и alerting.
Жизненный цикл	Владелец, change ticket, дата проверки и срок отключения.

07

АРХИТЕКТУРЫ РАЗВЕРТЫВАНИЯ

Карта точек наблюдения для ЦОД, филиалов, OT/ICS и гибридного облака

ГИБРИДНАЯ АРХИТЕКТУРА ВИДИМОСТИ

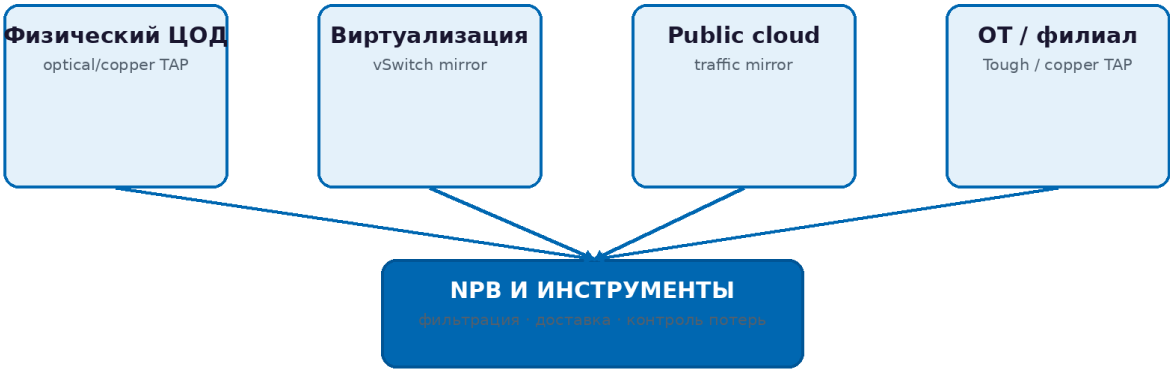


Рисунок 6. Разные источники трафика требуют единой модели coverage, capacity и ownership.

Как выбирать точку наблюдения

Определить защищаемый сервис, пользователей и тип инцидента, который требуется доказать.
Нанести маршруты north-south и east-west, включая резервные пути и asymmetric routing.
Отметить NAT, load balancer, firewall, proxy, VPN, MACsec и TLS termination.
Выбрать точку, где еще доступны нужные адреса, направление и payload либо необходимые метаданные.
Проверить, что один observation point действительно покрывает все ECMP/LAG/MLAG пути.
Зафиксировать владельца точки, maintenance window и downstream tool consumers.

Зона	Типовые точки	Ключевой вопрос
Интернет-периметр	До/после firewall, DDoS, load balancer	Нужны ли pre-NAT и post-policy копии?
ЦОД spine-leaf	Leaf uplinks, service leaf, inter-DC	Все ли ECMP пути покрыты?
Критичные серверы	Storage, database, identity, backup	Не остается ли traffic внутри host/vSwitch?
Филиал/WAN	Edge router, SD-WAN, Internet breakout	Где доступен незашифрованный context?
OT/ICS	Zone/conduit, control center, plant floor	Нужно ли industrial исполнение и пассивность?
Mobile core	N3/N6, GTP-U, PFCP/GTP-C	Как сохранить subscriber/session context?

Референс 1: филиал 1G copper

Компонент	Решение
Observation point	Между WAN/SD-WAN appliance и access switch.
TAP	Breakout copper, PoE pass-through при необходимости, redundant PSU и fail-to-wire.
Monitor	Два Rx-интерфейса локального recorder/NPB либо агрегирующий TAP при доказанном запасе.
Acceptance	Full duplex, IMIX/jumbo, PSU failure, PoE continuity и remote-tool outage.

Референс 2: ЦОД 100/400G

Компонент	Решение
Observation point	Leaf/spine, service insertion и inter-DC links с учетом ECMP.
TAP	Пассивный optical breakout, PMD/connector matched, расчет четырех optical paths.
Delivery	TAP→400G-capable NPB→100/25G tools, контроль Mpps, microbursts и FEC.
Acceptance	Rx power, DOM/FEC baseline, simultaneous full duplex, packet sequence и 24–72 h soak.

Референс 3: ОТ/ICS

Компонент	Решение
Observation point	Границы security zones/conduits, remote substations или production cell.
TAP	Пассивный optical или industrial copper с требуемыми environment ratings.
Security	Locked enclosure, Rx-only monitor path, отдельная management zone и data minimization.
Operations	Change control, запасной модуль, маркировка, remote hands и периодический loss baseline.

АРХИТЕКТУРНАЯ КАРТОЧКА

Для каждой площадки должна существовать одна схема с observation points, направлениями A/B, part numbers, split ratio, оптическими расчетами, NPB/tool destinations, owners и capacity. Словесного описания недостаточно.

Референс 4: virtual / cloud

Компонент	Решение
Coverage	Автоматическое включение workload по tags/policy и отчет об исключениях.
Transport	Mirror/vTAP→collector/NPB с расчетом MTU, bandwidth и failure domains.
Correlation	Cloud flow/log metadata, workload identity и UTC timestamp.
Acceptance	Scale-out, instance replacement, max frame, packet sequence и target failure.

Комплект результатов по площадке

- Схема observation points, резервных путей, NAT и точек шифрования.
- BOM с exact part numbers, optics, cables, licenses и spare units.
- Расчеты live/monitor capacity и оптического бюджета.
- Протокол PoC с raw counters, logs, packet sequence и измерениями отказов.
- Матрица owners, change/rollback procedure и support contacts.
- Baseline и thresholds, загруженные в систему эксплуатации.

08

БЕЗОПАСНОСТЬ И ШИФРОВАНИЕ

Monitor isolation, физическая защита, TLS/QUIC и жизненный цикл захваченных данных

Модель угроз ТАР-инфраструктуры

Угроза	Мера
Подключение несанкционированного приемника	Locked racks/panels, tamper evidence, inventory и контроль патч-кордов.
Инъекция через monitor-порт	Модель с подтвержденным Rx-only/data diode или независимая физическая защита.
Кража полного PCAP	RBAC, encryption at rest, retention, audit и отдельный forensic workflow.
Незаметное отключение одного направления	Per-port counters, alarms, test packets и регулярная сверка A/B.
Изменение cloud mirror policy	Four-eyes approval, config diff, tag coverage и SIEM audit.
Компрометация managed TAP	OOB management, AAA/MFA, firmware lifecycle, allow-list и backup config.

Шифрование: корректные ожидания

ТАР копирует зашифрованные пакеты без расшифровки. Для TLS 1.3 и QUIC packet capture сохраняет транспортные признаки, тайминг, размеры и доступную часть handshake, но не предоставляет application payload сам по себе.

Подход	Что дает	Риск / ограничение
Metadata-only	5-tuple, timing, sizes, TLS/QUIC fingerprints и certificates, если доступны	Нет содержимого приложения.
Reverse/forward proxy	Контролируемая TLS termination и L7 visibility	Trust, pinning, mTLS, latency и privacy.
Session key export	Расшифровка отдельных сессий без постоянного server key	Endpoint coverage и защита key material.
Passive decryption	Постфактум или real-time при доступных ключах	Не универсально; forward secrecy и key governance.
Endpoint/EDR telemetry	Context процесса и приложения	Агент, coverage, производительность и доверие к host.

NIST TLS 1.3

NIST SP 1800-37 рассматривает ТАР как источник зашифрованных пакетов, а дешифрацию — как отдельную архитектуру с key governance, session keys или middlebox [8]. Эти роли нельзя объединять в одном обещании «ТАР расшифровывает трафик».

Governance данных

Решение	Что зафиксировать	Владелец
Какие сегменты копируются	Scope, исключения, data classification	Security Architecture + data owners
Кто получает feed	Tool ports, accounts, network isolation	SOC / platform owner
Как сокращается payload	Filter, slicing, masking, metadata	Privacy/Compliance

Решение	Что зафиксировать	Владелец
Сколько хранится PCAP	Retention, deletion, legal hold	Legal/Compliance + service owner
Как сохраняются доказательства	Hash, time source, chain of custody	Incident response / forensics
Как аудируются изменения	Immutable logs, config diff, timestamps	Internal control / SOC

Временная синхронизация

Параметр	Минимальное требование
Точка timestamp	Ingress capture NIC/NPB/analyzer, указанная в архитектуре.
Источник	NTP, PTP IEEE 1588 и/или 1PPS; резервирование и holdover.
Погрешность	Численный допуск для correlation между инструментами.
Контроль	Offset, sync state, clock class, alarms и invalid-time marker.
Форензика	Time zone, UTC normalization и документированный clock evidence.

Security acceptance

- ☐ Физический доступ к ТАП, панелям и monitor-портам ограничен и журналируется.
- ☐ Rx-only/data-diode свойство подтверждено datasheet и испытанием, если оно обязательно.
- ☐ Управляемые компоненты используют OOB, AAA/MFA, RBAC и аудит конфигурации.
- ☐ Scope, minimization, retention, deletion и legal hold согласованы владельцами данных.
- ☐ Time source, offset alarms и формат evidence проверены совместно с IR/forensics.
- ☐ Экспорт PCAP и ключевого материала имеет отдельный утвержденный workflow.

Карточка потока данных

Поле	Решение
Источник / категории данных	_____
Получатели / purpose	_____
Фильтрация / slicing / masking	_____
Retention / deletion / legal hold	_____
Владелец / согласование	_____

09

ВЫБОР РЕШЕНИЯ И RFP

Нейтральная оценочная модель, продуктовые примеры и проверяемые требования

Оценочная модель

Группа	Вес	Примеры критериев
Физическая совместимость	20%	Media, PMD, connector, polarity, split ratio, optical budget.
Достоверность monitor-path	20%	Breakout, errors, direction, line rate, Mpps, drops counters.
Надежность	15%	Passive continuity, PSU, fail-to-wire, link behavior, environment.
Безопасность	10%	Rx-only, no IP/passive, AAA/audit for managed models, physical security.
Масштаб и плотность	10%	Taps per RU, cable management, regeneration/NPB integration.
Эксплуатация	10%	Labeling, replaceability, DOM/counters, documentation, support.
TCO и lifecycle	15%	Hardware, optics, cross-connects, spare units, support и upgrade path.

ПРАВИЛО RFP

Требование без метода проверки остается пожеланием. Для каждого обязательного пункта укажите evidence: datasheet, измерение power meter, packet test, failure test, configuration export или внешний analyzer.

Ключевые вопросы поставщику

Область	Вопрос
Совместимость	Какой точный PMD, wavelength, connector, fiber и lane architecture поддерживаются?
Оптика	Каковы actual network/monitor insertion loss и допуски для каждого split ratio?
Errors	Какие errored frames видны monitor receiver и чем это подтверждено?
Aggregation	Каково поведение при sum A+B > monitor capacity и где видны drops?
Copper	Каковы fail-to-wire gap, renegotiation, PoE limits и behavior при восстановлении питания?
Security	Является ли monitor port физически Rx-only и как это реализовано?
Lifecycle	EoS/EoL, replacement part, roadmap 400/800G и warranty?
Quality	Какие factory tests и serial-level acceptance data доступны?

Продуктовые примеры Keysight

Следующая таблица иллюстрирует классы решений и не заменяет актуальный конфигуратор. Характеристики подтверждаются выбранным part number, datasheet и коммерческой спецификацией.

Пример	Опубликованные ориентиры	Проверить в проекте
Flex Tap II	Пассивные SM/MM, 1G–400G, split 50/50–90/10, до 24 TAP в 1U [10].	PMD, connector, actual insertion loss, module density.
Flex Tap VHD	Портфель указывает до 36 TAP в 1U для соответствующей платформы [9].	Доступные модули, cable management и serviceability.

Пример	Опубликованные ориентиры	Проверить в проекте
IxTap Copper	10/100/1000, fail-to-wire, redundant power, PoE/jumbo, air-gapped monitor [11].	Firmware/revision, PoE class, failure gap и management mode.
Patch Tap	Пассивная точка доступа, интегрированная в patching [12].	Loss, supported fiber/connector, rack/cross-connect design.
Tough Tap	Варианты для industrial/ICS и удаленных площадок [13].	Environmental rating, certification, media и maintenance.

Shortlist readiness

- ☐ Одинаковые требования применены ко всем поставщикам.
- ☐ Получены exact part numbers и полная BOM с оптикой, chassis и spare units.
- ☐ Оптические расчеты выполнены по actual insertion loss, а не только по split ratio.
- ☐ Поставщик принял единую методику PoC и критерии FAIL.
- ☐ Проверены lifecycle, гарантия, совместимость и migration path.
- ☐ Все отклонения внесены в risk register до коммерческого сравнения.

Иерархия доказательств

Уровень	Пример	Вес при решении
1. Приемочный PoC	Raw analyzer results, power, counters, failure tests	Максимальный
2. Контракт	Спецификация, SLA, warranty, lifecycle letter	Высокий
3. Datasheet / release notes	Точная модель, revision и поддерживаемый режим	Высокий
4. Factory / independent report	Serial-level или независимое испытание	Средний
5. Demo / презентация	Сценарий поставщика без единой методики	Ориентир

Нормализация коммерческих предложений

Категория	Сравнивать на одинаковом горизонте
CAPEX	Chassis/modules, optics, cables, panels, licenses и installation.
Поддержка	Срок, SLA, advanced replacement, software access и обучение.
Резерв	Spare ratio, время замены, совместимость ревизий и stock risk.
Lifecycle	EoS/EoL, migration path, roadmap и повторный PoC.
Риск	Окно монтажа, downtime, недоказанная емкость и blind spots.

10

РОС И ПРИЕМКА

Внешний analyzer, полный duplex, microbursts, error handling и тесты отказа

Принципы честного испытания

- Зафиксировать topology, hardware revision, firmware, optics, split ratio и configuration.
- Использовать внешний traffic generator/analyzer и sequence numbers, а не только счетчики тестируемого устройства.
- Проверять оба направления одновременно на 64/128/256/512/1024/1518 bytes, jumbo и IMIX.
- Проводить positive и negative tests: overload, loss of power, tool outage, wrong MTU и optical margin boundary.
- Сохранять raw results, counters, logs, power readings и фотографии маркировки.
- Повторить критические тесты после любого изменения firmware, optics или topology.

Обязательная программа

ID	Тест	Нагрузка / действие	Критерий
T01	Baseline live-path	Линк, latency, counters до/после вставки	Нет необъясненного влияния
T02	Full duplex	Line rate A→B и B→A одновременно	0 unexplained monitor loss
T03	Small packets	64/128 B, max Mpps	Заявленная packet capacity
T04	IMIX/jumbo	Реальный профиль + max frame	Без truncation/alteration
T05	Microbursts	Короткие пики обоих направлений	Drops/counters объяснимы
T06	Direction	Маркированные A/B flows	Нет перепутанных направлений
T07	Errors	FCS/runts/giants при наличии генератора	Результат соответствует заявлению
T08	Optical power	Все четыре тракта	Запас и overload в допуске
T09	Aggregation overload	$\Sigma A+B > egress$	Поведение и counters документированы
T10	PSU failure	Каждый PSU и полное питание	Gap в пределах требования
T11	Tool outage	Down/slow/disconnected monitor	Live-path не затронут
T12	Soak	24–72 h mixed traffic	Нет скрытой деградации

Оптический протокол измерений

Измерение	До ТАР	После ТАР	Допуск / вывод
Rx power A	_____ dBm	_____ dBm	_____
Rx power B	_____ dBm	_____ dBm	_____
Monitor A	—	_____ dBm	_____
Monitor B	—	_____ dBm	_____
FEC corrected	_____	_____	_____
FEC uncorrectable	_____	_____	_____
CRC / link events	_____	_____	_____

Критерии приемки

Показатель	Согласованное значение
Monitor packet loss	0 необъясненных потерь при указанном traffic profile и duration
Duplicates / reorder	0 либо документированное ожидаемое значение aggregation/mirroring
Live-path gap при отказе	_____ мс / _____ пакетов
Optical margin	Не менее _____ дБ для каждого тракта
FEC/CRC delta	Не превышает baseline/согласованный порог
Timestamp accuracy	Не хуже _____ нс/мкс/мс при указанном time source
Soak duration	_____ часов без unexplained degradation

PASS/FAIL

Если критерий не имеет числа, профиля нагрузки и метода измерения, он не годится для приемки. Формулировка «работает штатно» должна быть заменена измеренным evidence.

Негативные сценарии

Сценарий	Ожидаемое evidence
Aggregation overload	Drops/queues видимы; live-path не затронут; результат объясним.
Tool slow/down	Monitor congestion локализован; production continuity сохранена.
Wrong MTU	Truncation/drop обнаружены счетчиками и максимальным test frame.
Power loss/recovery	Измерены оба gap, link events, PoE и восстановление monitor.
Optical boundary	Rx/DOM/FEC подтверждают согласованный margin без overload.

Пакет доказательств

- ☐ Topology, BOM, hardware/firmware revisions и конфигурация.
- ☐ Traffic profiles, sequence results, drops/reorder/duplicates и raw counters.
- ☐ Tx/Rx, insertion loss, DOM, FEC/CRC и фотографии маркировки.
- ☐ Failure-test timeline с миллисекундами, пакетами и состояниями линка.
- ☐ Подписанные deviations, risk acceptance, rollback и итоговый PASS/FAIL.

11

ЭКСПЛУАТАЦИЯ И ЭКОНОМИКА

Baseline, мониторинг, диагностика, роли, TCO и инвестиционное решение

Что передать эксплуатации

Артефакт	Содержание
Схема	Observation point, A/B directions, ports, fibers, split ratio, NPB/tools.
Паспорт линии	PMD, optics, Tx/Rx, loss budget, DOM/FEC baseline и serial numbers.
Acceptance report	Traffic profiles, loss/reorder, failure gaps, raw logs и photos.
Runbook	Normal state, alarm thresholds, troubleshooting и rollback.
Inventory	TAP modules, chassis, spare units, patch cords и support contacts.
Ownership	Network, cabling, SOC, tool owner, change manager и vendor support.

Регулярные проверки

Период	Проверка
Постоянно	Monitor link, packet rate, drops, NPB queues, tool health и time sync.
Ежемесячно	Сверка A/B traffic, alarms, inventory и configuration changes.
Ежеквартально	Capacity peak/Mpps, DOM/FEC trend, patching и spare readiness.
Ежегодно	Failure tests, optical cleaning/inspection, RFP assumptions и lifecycle.
После изменения	Regression для affected observation point и обновление baseline.

Диагностика

Симптом	Вероятная причина	Проверка
Не поднимается live-link	PMD/polarity, low Rx, dirty connector, negotiation	DOM/power, swap known-good, endpoint counters
Не видно одного направления	Перепутаны A/B, fiber lane, monitor Rx	Маркированный test flow и physical trace
Drops только на tool	Tool/NIC/storage overload	NPB egress, NIC ring, CPU/disk counters
Drops при aggregation	$\Sigma A+B >$ egress или microburst	Peak/Mpps, queues, watermarks
Рост FEC/CRC после ТАП	Недостаточный margin/загрязнение	Power meter, DOM/FEC, clean/inspect
Дублированные пакеты	Несколько observation points или SPAN Rx+Tx	Sequence trace и source mapping
Неверное время	Unsynced capture point/clock	PTP/NTP state, offset и timestamp location

RACI

Процесс	Ответственный	Согласование
Observation points и capacity	Network Architecture	Service owners, SOC
Оптический расчет и монтаж	DC/CKC team	Network owner
Security feeds и retention	SOC / Security Architecture	Privacy/Legal
NPB/tool capacity	Visibility platform owner	Tool owners
Failure tests	Operations / project team	Service owner и Change Board
Firmware/lifecycle	Platform owner	Vendor support и ИБ

TCO

Категория	Статьи затрат
Оборудование	TAP modules/chassis, copper units, secure/industrial options и spares.
Оптика и CKC	Transceivers, fibers, MPO/LC, panels, cross-connects и монтаж.
Monitor infrastructure	NPB ports, capture NICs, tool licenses, storage и time source.
Внедрение	Design, maintenance window, lab/PoC, installation и training.
Эксплуатация	Support, cleaning, inventory, monitoring, recertification и changes.
Риск	Downtime during install, insufficient margin, EoL migration и blind spots.

Сравнение инвестиций TAP и SPAN

Фактор	TAP	SPAN
Начальные затраты	Оборудование, оптика, монтаж и окно	Свободный switch port и инженерное время
OPEX	Низкий для passive, но нужен monitor-chain	Config, drift, повторное включение и platform limits
Риск доказательности	Ниже при корректном PoC	Зависит от platform/load/session
Масштабирование	Chassis/NPB/cabling	Ports/sessions/fabric/tunnels
Наилучший сценарий	Постоянные критические точки	Временная диагностика и low-risk links

ИНВЕСТИЦИОННОЕ РЕШЕНИЕ

Сравнивайте не цену порта, а стоимость гарантированного результата: coverage, сохранность пакетов, время расследования, риск изменения production-конфигурации и срок эксплуатации архитектуры.



МАТРИЦА ТРЕБОВАНИЙ RFP

Заполняемый фрагмент для закупочной документации

ID	Приоритет	Требование	Проверка	Ответ
R-01	Обяз.	Exact media/PMD/connector/polarity соответствуют линии	Datasheet + inspection	
R-02	Обяз.	Actual network/monitor insertion loss указан	Datasheet + power test	
R-03	Обяз.	0 unexplained monitor loss при согласованной нагрузке	PoC T02-T05	
R-04	Обяз.	Breakout сохраняет направления A/B	PoC T06	
R-05	Обяз.	Aggregation overload behavior и counters документированы	PoC T09	
R-06	Обяз.	Failure behavior соответствует live-path SLA	PoC T10-T11	
R-07	Обяз.	Rx-only/data diode подтвержден, если требуется	Datasheet + test	
R-08	Обяз.	PoE/jumbo/negotiation поддержаны для copper	PoC + datasheet	
R-09	Обяз.	Документированы environment ratings и warranty	Certificates	
R-10	Желат.	Модульная плотность и front-serviceability	Inspection	
R-11	Желат.	Интеграция с NPB и единые alarms	Demo/API	
R-12	Инфо	Roadmap 400/800G и lifecycle 5 лет	Письмо производителя	

В ПРОТОКОЛ РОС

Форма фиксации конфигурации, нагрузки и результата

Параметр	Значение
Площадка / линия	
Поставщик / модель / part number	
Serial / hardware revision	
Firmware / management mode	
Media / PMD / connector	
Split ratio / insertion loss	
Network optics / monitor optics	
Traffic generator/analyzer	
Traffic profile / duration	
Схема / номера портов	
Ограничения / исключения	

Итоговая ведомость

Test ID	PASS	FAIL	Фактический результат / evidence
T01	☐	☐	
T02	☐	☐	
T03	☐	☐	
T04	☐	☐	
T05	☐	☐	
T06	☐	☐	
T07	☐	☐	
T08	☐	☐	
T09	☐	☐	
T10	☐	☐	
T11	☐	☐	
T12	☐	☐	



ЧЕК-ЛИСТ ПРИЕМКИ

Подписи выдаются после проверки физического тракта, пакетов, отказов и документации

- ☐ Фактическая модель, hardware revision, firmware и BOM соответствуют проекту.
- ☐ Network/monitor insertion loss и split ratio подтверждены документами и измерениями.
- ☐ Оба live-path и оба monitor-path имеют согласованный оптический запас.
- ☐ Полнодуплексный тест, IMIX, small packets, jumbo и microbursts завершены.
- ☐ Направления A/B однозначно маркированы и проверены test flows.
- ☐ Aggregation overload и downstream tool congestion имеют видимые counters/alarms.
- ☐ Power failure, restoration и tool outage не нарушают live-path сверх допуска.
- ☐ Monitor isolation, физическая защита и management hardening подтверждены.
- ☐ Схемы, baseline, runbook, support contacts и spares переданы эксплуатации.
- ☐ Retention, доступ к PCAP и владельцы данных согласованы.

Роль	ФИО	Решение / подпись / дата
Сетевой архитектор		
СКС / оптическая инфраструктура		
Информационная безопасность		
Эксплуатация		
Владелец сервиса		
Руководитель проекта		



ГЛОССАРИЙ

Термины физического доступа и сетевой видимости

Термин	Определение
TAP	Специализированная точка получения копии сетевого трафика.
Test Access Port/Point	Распространенные варианты расшифровки термина TAP.
Live-path	Рабочий путь production traffic между сетевыми узлами.
Monitor-path	Путь копии трафика от TAP до инструмента.
Breakout	Раздельный вывод направлений A→B и B→A.
Aggregation	Объединение направлений или источников на одном monitor-egress.
Regeneration	Создание нескольких идентичных копий одного feed.
Split ratio	Доля оптической мощности, направляемая в network и monitor legs.
Insertion loss	Потери мощности, вносимые компонентом в оптический тракт.
Optical margin	Запас между полученной мощностью и минимальной чувствительностью Rx.
PMD	Physical Medium Dependent — конкретная физическая реализация Ethernet-интерфейса.
PAM4	Четырехуровневая амплитудная модуляция, используемая в высокоскоростных интерфейсах.
FEC	Forward Error Correction — коррекция ошибок на физическом/PCS уровне.
DOM/DDM	Цифровой мониторинг параметров оптического трансивера.
SPAN	Зеркалирование трафика средствами коммутатора.
ERSPAN	Удаленное зеркалирование с инкапсуляцией через IP/GRE.
vTAP	Программный или виртуальный источник копии workload traffic.
NPB	Network Packet Broker — фильтрация, преобразование и доставка копий инструментам.
Data diode	Физическое ограничение передачи в одном направлении.
Fail-to-wire	Сохранение электрического соединения network ports при отказе активного TAP.
Fail-open	При отказе inline-функции production traffic продолжает проходить.
Mpps	Миллионы пакетов в секунду.
IMIX	Смесь размеров пакетов, приближенная к реальному трафику.
Soak test	Продолжительное испытание смешанной нагрузкой для выявления скрытой деградации.



ИСТОЧНИКИ

Стандарты и актуальные официальные материалы, проверенные при подготовке документа

[1] IEEE 802.3df-2024 — 800 Gb/s and 1.6 Tb/s Ethernet

<https://standards.ieee.org/ieee/802.3df/11107/>

[2] Cisco — Introduction to Optical Fibers, dB, Attenuation and Measurements

<https://www.cisco.com/c/en/us/support/docs/optical/synchronous-digital-hierarchy-sdh/29000-db-29000.html>

[3] Cisco — Passive Optical Networks: Cabling Considerations

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-pon-series/nb-06-cat-pon-wp-cte-en.html>

[4] Keysight — Ixia Flex Taps: Insertion Loss Data

<https://www.keysight.com/us/en/assets/7019-0292/technical-overviews/Flex-Tap-Insertion-Loss-Calculator.pdf>

[5] Cisco Catalyst — Switch Port Analyzer (SPAN)

<https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/mgmt/management-configuration-guide/span.html>

[6] Cisco Nexus 9000 — Switched Port Analyzer

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/106x/config-guides/sys-mgmt/cisco-nexus-9000-series-nx-os-system-management-configuration-guide-release-106x/m-configuring-span.html>

[7] AWS — Traffic Mirroring limitations

<https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-network-limitations.html>

[8] NIST SP 1800-37 — Addressing Visibility Challenges with TLS 1.3

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-37.pdf>

[9] Keysight — Network Taps portfolio

<https://www.keysight.com/us/en/products/network-visibility/network-taps.html>

[10] Keysight — Flex Tap II

<https://www.keysight.com/us/en/assets/3122-2120/data-sheets/Flex-Tap-II.pdf>

[11] Keysight — IxTap Copper Tap

<https://www.keysight.com/us/en/assets/3120-1421/data-sheets/IxTap-Copper-Tap.pdf>

[12] Keysight — Patch Taps

<https://www.keysight.com/us/en/products/network-visibility/network-taps/patch-taps.html>

[13] Keysight — Tough Taps

<https://www.keysight.com/us/en/products/network-visibility/network-taps/tough-taps.html>

[14] Keysight — Difference between Network TAP and SPAN Port

<https://www.keysight.com/us/en/library/demos/product-tour/difference-between-network-tap-and-span-port.html>

[15] RFC 8446 — TLS 1.3

<https://www.rfc-editor.org/info/rfc8446>

[16] RFC 9000 — QUIC

<https://www.rfc-editor.org/info/rfc9000>

АКТУАЛЬНОСТЬ

Источники проверены в августе 2026 года. Перед закупкой необходимо повторно проверить текущие datasheet, release notes, compatibility matrix, part numbers и коммерческую спецификацию.