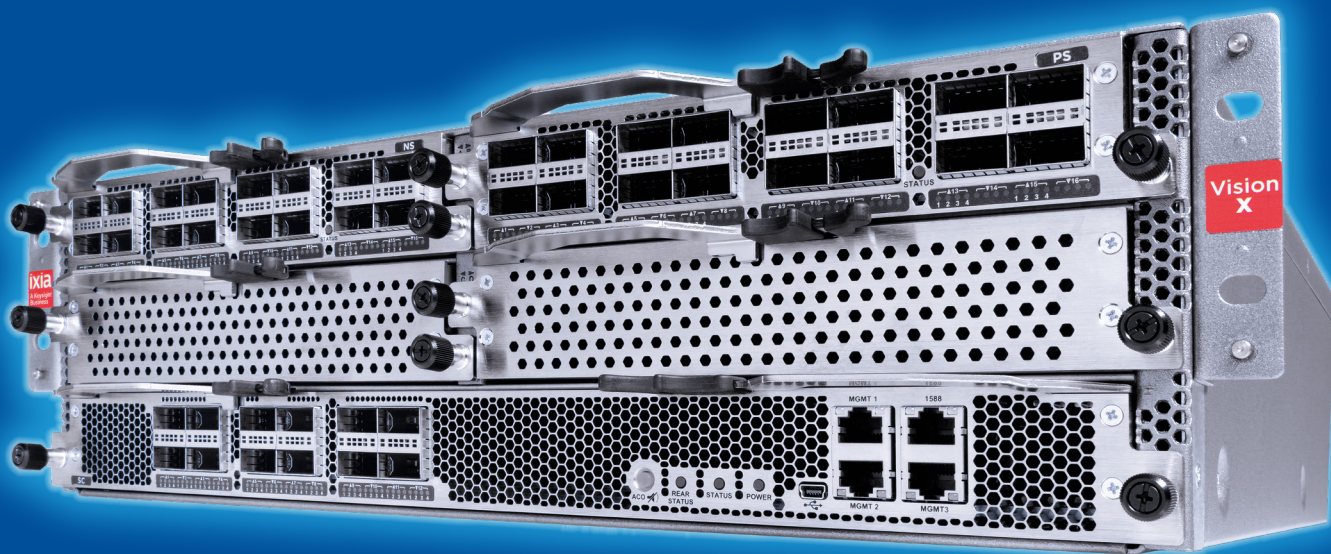




ixia | A Keysight
Business



ПРОДУКТЫ KEYSIGHT

для сетевой видимости

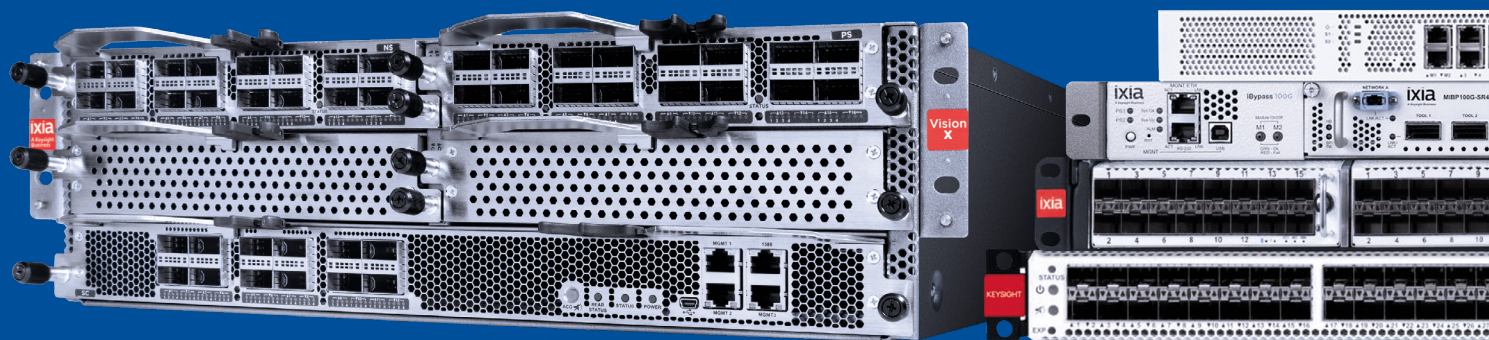
СОДЕРЖАНИЕ

02	Введение
04	Брокеры сетевых пакетов (Packet Brokers)
12	Обходные коммутаторы (Bypass Swithes)
14	Сетевые ответвители (Network Taps)
18	Централизованное управление видимостью (KVO)
20	Платформа активного мониторинга (HAWKEYE)
22	Синхронизация времени (Timekeeper)

ВВЕДЕНИЕ

ОБЕСПЕЧИВАЙТЕ СВЯЗЬ И БЕЗОПАС- НОСТЬ МИРА

с помощью динамической
сетевой аналитики





Потребность в постоянно работающих сетях повсеместна, и ожидания высоки, когда речь идет о поддержании их связи и безопасности. По мере развития технологий периферийные вычисления, облачные среды, сложные угрозы безопасности, растущие требования к пропускной способности и строгие нормативные требования затрудняют извлечение полезной информации из вашей сети.

Заказчики полагаются на решения Keysight для получения подробных данных о сетевом трафике, приложениях и пользователей в любой сетевой среде. Это глубокое понимание мы называем динамической сетевой аналитикой. Оно помогает вам постоянно внедрять инновации, соблюдать жесткие соглашения об уровне обслуживания и обеспечивать бесперебойную и безопасную работу приложений.

Предоставление динамической сетевой аналитики зависит от сетевой видимости, и Keysight предлагает полный набор

продуктов. Брокеры сетевых пакетов Keysight Vision (NPB) находятся в основе. Они помогают вам максимально эффективно использовать ваши инструменты безопасности и мониторинга сети, предоставляя отфильтрованный, оптимизированный трафик.

Внешние байпасные переключатели, такие как Keysight iBypass, обеспечивают высокую доступность и отказоустойчивость встроенных устройств, чтобы ваша сеть оставалась в сети. А сетевые ответвители (taps) обеспечивают чистое и неизменное представление о трафике в сети, формируя основу динамической сетевой аналитики.

Вместе продукты Keysight для сетевой видимости позволяют вам и всем вашим сетевым инструментам работать более эффективно и результативно, чтобы вы могли поддерживать высокую производительность и строгую безопасность.



БРОКЕРЫ СЕТЕВЫХ ПАКЕТОВ (PACKET BROKERS)



Узнать больше о том что
делают брокеры сетевых
пакетов и зачем они нужны:



Правильные данные для правильных инструментов



NPB являются центральным элементом обеспечения динамической сетевой аналитики в вашей сети. Используя фильтрацию трафика с учетом приложений, расшифровку и дедупликацию, NPB позволяют вашим инструментам безопасности и мониторинга работать более эффективно и результативно, гарантируя, что каждый инструмент получает правильные данные — не больше и не меньше. Более того, в отличие от многих конкурентных предложений, NPB от Keysight предлагают аппаратное ускорение на базе программируемых пользователем вентильных матриц (FPGA). Эта функциональность является ключевым фактором для любого развертывания средств видимости, поддерживающего критически важную безопасность или мониторинг сети, поскольку она позволяет применять функции и фильтры на линейной скорости без потери трафика, «слепых зон» или отбрасывания пакетов. Потому что частичная видимость — это недостаточно хорошо.

NPB от Keysight предлагают следующие ключевые функции:

- Архитектура с нулевой потерей пакетов
- Балансировка нагрузки для нескольких инструментов мониторинга или безопасности
- Централизованное расшифрование, включая расширенный TLS 1.3.
- Динамический компилятор фильтров снижает операционную сложность
- Простой в использовании графический пользовательский интерфейс (GUI)

Видимость для финансов

Узнать больше
о TradeVision:



Keysight TradeVision — это уникальный продукт для организаций финансовых услуг. Он сочетает мониторинг состояния рыночных каналов с функциональностью, позволяющей отслеживать 240 миллионов сообщений о сделках/котировках в секунду. Это в 12 раз больше, чем на объединенных рынках акций и опционов США. Благодаря аппаратному ускорению на базе FPGA без потери данных, точной отметке времени и возможностям агрегации ответвителей (tap), TradeVision сокращает время, необходимое для устранения потенциально дорогостоящих проблем.

Дополнительные функции включают следующее:

- Обнаружение мультикаст-разрывов
- Расширенная аналитика задержек
- Оповещение о микровсплесках
- Статистика трафика с высоким разрешением
- Упрощенное управление каналами

Стеки функций ВИДИМОСТИ

Расширенная обработка пакетов и интеллектуальная контекстно-зависимая фильтрация

Надежные стеки функций интеллектуальной видимости Keysight помогают вам максимально эффективно использовать брокеры сетевых пакетов Vision Series и всю вашу платформу видимости и безопасности. Эти программные стеки обеспечивают фильтрацию на основе уровней L2–L7. Каждый стек функций

имеет целенаправленную конструкцию, чтобы гарантировать вам наилучшую производительность, будь то в физическом центре обработки данных или в частном, гибридном или публичном облаке.

Стеки функций NPВ обеспечивают динамическую сетевую аналитику, которая расширяет и улучшает функциональность NPВ с помощью расширенной обработки пакетов.

NetStack

Обеспечивает золотой стандарт базового уровня для сетевой видимости. Включает надежную фильтрацию, балансировку нагрузки, агрегацию, репликацию и многое другое с тремя этапами фильтрации (входной, динамической и выходной) и динамическим компилятором фильтров.

[Узнать больше
о NetStack](#)



PacketStack

Обеспечивает интеллектуальную фильтрацию, обработку и транспортировку пакетов с дедупликацией, которая удаляет дублирующиеся пакеты на полной линейной скорости без потерь. Другие возможности включают удаление заголовков (протоколов), обрезку пакетов, проставление временных меток, маскирование данных и защиту от всплесков.

С помощью PacketStack вы можете делать следующее:

- Защищать и продлевать срок службы инструментов мониторинга, чтобы они работали более эффективно.
- Повышать производительность инструментов, сохраняя только необходимые байты заголовков и обрезая полезную нагрузку до настраиваемой пользователем длины.
- Скрывать личную идентифицируемую информацию, такую как номера кредитных карт и номера социального страхования, перед отправкой данных в инструменты анализа.
- Измерять задержку инструментов мониторинга с наносекундным разрешением и точностью, проставляя временные метки на всех пакетах для чувствительных ко времени приложений.
- Завершать туннели L2GRE или ERSPAN от vTap и передавать обычный Ethernet-трафик вашим инструментам.
- Удалять новые или проприетарные протоколы, такие как L3GRE, Jmirror, PBB-TE, LISP, VSL, OTV и PPPoE, используя универсальное удаление заголовков Удалять новые или проприетарные протоколы, такие как L3GRE, Jmirror, PBB-TE, LISP, VSL, OTV и PPPoE, используя универсальное удаление заголовков

[Узнать больше
о PacketStack](#)



SecureStack

Оптимизирует обработку защищенного трафика и поддерживает встроенное и выносное (внеполосное) дешифрование SSL/TLS. Data Masking Plus соответствует требованиям Закона о переносимости и подотчетности медицинского страхования, Индустрии платежных карт и другим нормативным требованиям. Достигайте большей видимости, расшифровывая трафик для быстрого обнаружения скрытых вредоносных программ и предотвращения потери данных или узких мест в инструментах безопасности.

[Узнать больше
о SecureStack](#)



MobileStack

Предлагает интеллектуальную видимость для эволюционного пакетного ядра мобильного оператора с протоколом туннелирования General Packet Radio Service, или GPRS Tunneling Protocol (GTP). MobileStack обеспечивает корреляцию протокола инициации сеансов (SIP) и балансировку нагрузки, фильтрацию по конкретному абоненту, списки разрешенных абонентов и выборку абонентов. MobileStack на Vision X может коррелировать до 512 миллионов абонентских сессий и 1600 ГБ трафика пользовательской плоскости на шасси; поддерживает производительность 5G.

[Узнать больше
о MobileStack](#)

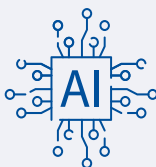


AIStack

AI Stack — это решение для обеспечения полной видимости использования AI/ML и generative AI в корпоративной сети. Оно позволяет отслеживать, где и как применяются AI-приложения, выявлять несанкционированное использование и анализировать трафик на уровне приложений. За счёт Deep Packet Inspection (DPI), работы с зашифрованным и открытым трафиком, а также сигнатурного анализа достигается высокая точность обнаружения. Это даёт возможность контролировать риски, связанные с безопасностью данных, приватностью и соответствием требованиям регуляторов.

Решение использует продвинутые механизмы дешифрования, session-aware анализ и динамические сигнатуры для глубокого понимания поведения AI-приложений. Оно позволяет анализировать запросы, ответы и передаваемые данные, включая мультимедиа и пользовательские файлы. Такой уровень прозрачности помогает выявлять утечки данных, аномалии и потенциальные угрозы в реальном времени. В результате компании получают инструмент для безопасного внедрения AI, повышения доверия и оптимизации использования технологий.

[Узнать больше
о AIStack](#)



AppStack

Обеспечивает контекстно-зависимую фильтрацию на прикладном уровне, основанную на сигнатурах, с точной и быстрой идентификацией приложений, геолокацией и маркировкой, запатентованным обнаружением сигнатур и опциональным использованием регулярных выражений (Regex) фильтрации. Простой интерфейс управления с помощью указателя и щелчка мыши позволяет вам выбирать интересные типы прикладного трафика и фильтровать трафик для инструментов. AppStack улучшает платформы мониторинга, добавляя более богатый набор географической, прикладной и устройственной информации.

[Узнать больше
о AppStack](#)



TradeStack

Предлагает финансовым рынкам капитала упрощенный инструмент управления данными рыночных каналов, который устраняет сложности настройки, анализа и управления данными рыночных каналов. Функции включают статистику трафика с высоким разрешением до 0,1 мс, обнаружение микровсплесков, работоспособность канала, измерение задержки и обнаружение разрывов.

С помощью модульных стеков NPB от Keysight вы можете добавлять только те возможности и функции, которые вам нужны, именно тогда, когда они вам нужны. Оснащение ваших NPB полным стеком программных решений гарантирует, что ваша архитектура сетевой видимости будет развиваться и масштабироваться для поддержки текущих и будущих потребностей.

[Узнать больше
о TradeStack](#)



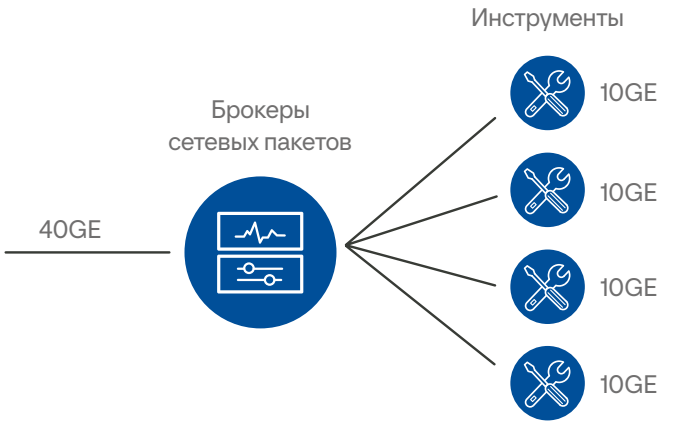
Остановите хакеров с помощью обработки защищенного трафика и дешифрования SSL/TLS

Чтобы предотвратить слепые зоны, вам необходимо видеть весь сетевой трафик — как дешифрованный, так и зашифрованный. Но та же самая шифрация, которая используется для защиты ваших данных, может быть обоюдоострым мечом. Киберпреступники могут атаковать вашу сеть, скрывая программы-вымогатели и вредоносное ПО внутри зашифрованных данных, подобно троянскому коню. Победите хакеров в их же игре, переложив ресурсоемкую задачу дешифрования SSL/TLS на NPB Vision Series с SecureStack. Это повысит эффективность работы ваших инструментов, не перегружая их и не влияя на их производительность.



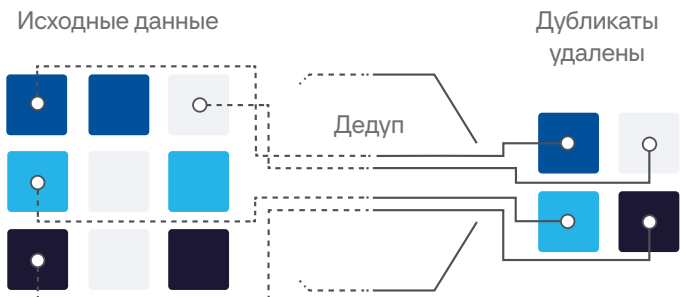
Сократите расходы и продлите срок службы инструментов с помощью балансировки нагрузки

NPB Vision с NetStack выполняют агрегацию и балансировку нагрузки, разбивая данные на потоки с меньшей скоростью для отправки соответствующим инструментам. Например, распределение 40 Гбит/с трафика между несколькими инструментами на 10 Гбит/с продлевает срок службы ваших инструментов на 10 Гбит/с до тех пор, пока у вас не появится бюджет на более дорогие инструменты, поддерживающие более высокие скорости передачи данных.



Дедупликация повышает эффективность

инструментов мониторинга и безопасности на 35% до 50% за счет уменьшения объема фильтрованного трафика, отправляемого инструментам.



Следующее поколение брокеров сетевых пакетов: Vision 400 и E400S



Масштабируйте вашу видимость до скорости 400G.

Keysight Vision 400 и Vision E400S — это решения для сетевой видимости следующего поколения. Обладая комплексными наборами функций, они удовлетворяют постоянно меняющиеся потребности в видимости вашей производственной сети для сетевых скоростей до 400 Гбит/с.

Будучи очень компактными и имеющими размер 1RU, их передние панели предоставляют 24 порта QSFP56 и 16 портов QSFP-DD. Каждый QSFP-DD может быть разветвлен на множество портов меньшей скорости (200G, 100G, 40G, 50/25/10G) с помощью разветвляющих кабелей. Это единственные NPB, которые поддерживают все возможные комбинации скоростей, что увеличивает возможность взаимодействия с устаревшими устройствами, максимизируя при этом гибкость проектирования.

Перепрограммируемая природа кремния обеспечивает быструю реализацию нового парсера или опции удаления заголовков любых новых протоколов, известных или проприетарных. Новые опции балансировки нагрузки (LB) поддерживают балансировку нагрузки на группу портов. В дополнение к традиционной сессионно-зависимой балансировке нагрузки

новые опции позволяют асимметричную LB, взвешенную LB, случайную LB и LB с использованием заголовка туннелированного IP.

Vision 400 содержит высокопроизводительную FPGA, которая обеспечивает дополнительные возможности PacketStack сверх возможностей E400S, такие как дедупликация на линейной скорости, обрезка пакетов и защита от всплесков.

Основные характеристики:

- Компактный NPB размером 1RU, поддерживающий скорости портов 10 / 25 / 40 / 50 / 100 / 200 / 400G
- Программируемый кремний на основе P4 и Tofino
- Полнодуплексная неблокируемая L2-коммутация на линейной скорости 9,2 Тбит/с
- Временная метка на входе с наносекундным разрешением с использованием PTP/NTP и входов синхронизации PPS
- Единственный в отрасли NPB на 400G, поддерживающий все комбинации скоростей QSFP-DD: 1×400G, 2×200G, (1,2,4)×100G, (4,8)×50G, (1,2)×40G, 8×25G, 8×10G.

Продукт	Vision 400	Vision X	Vision ONE	Vision E400S	Vision 7816	Vision Edge 10
Описание	Масштабируемое шасси 1RU, поддерживающее стеки интеллектуальной видимости для сетей 10/25/40/50/100/200/400G	Высокопроизводительное, высокой плотности, модульное, масштабируемое шасси 3RU для сетей 10/25/40/50/100G	Полнофункциональное готовое решение с видимостью 10/40G в факторе 1RU	Масштабируемое шасси 1RU для сетей 10/25/40/50/100/200/400G	Масштабируемое высокоплотное шасси 2RU, поддерживающее сети 10/25/50/100G	Экономичная высокоплотная видимость на уровне стоек для сетей 10/25/40/50/100G
Архитектура с нулевой потерей пакетов	•	•	•	•	•	•
Динамический компилятор фильтров	•	•	•	•	•	•
Высота системы (RU)	1	3	1	1	2	1
Расширенная обработка пакетов	•	•	•	•		
Проставление временных меток на входящем порту для последующей обработки	•					
АС резервный источник питания (горячая замена)	•	•	•	•	•	•
DC резервный источник питания (горячая замена)	•	•	•	•	•	•
Макс. пропускная способность обратной панели (Гбит/с)	9200	6400	640	9200	6400	3200
Макс. кол-во портов 1G	0	0	64	0	0	0
Макс. кол-во портов 10G	152	108	64	152	128	128
Макс. кол-во портов 25G	152	108	0	152	128	128
Макс. кол-во портов 40G	32	76	16	32	64	32
Макс. кол-во портов 50G	152	108	0	152	128	64
Макс. кол-во портов 100G	64	60	0	64	64	32
Макс. кол-во портов 400G	16	0	0	16	0	0
	Перейти к Vision 400	Перейти к Vision X	Перейти к Vision ONE	Перейти к Vision E400S	Перейти к Vision 7816	Перейти к Vision Edge 100
Узнать больше						

Продукт	Vision Edge 40	Vision Edge 10S	Vision Edge 1S	Vision Edge OS	Vision T1000	TradeVision
Описание	Экономичная видимость на уровне стойки для 1/10/40G	Идеально подходит для развертываний на удаленных площадках, поддерживающих сети 1/10G	Компактная экономичная видимость для филиальных площадок	Деагрегированная операционная система видимости для открытого коммутационного оборудования	Прочный NPB, предназначенный для суровых условий эксплуатации, рабочая температура от -40°C до +85°C	Мониторинг рыночных каналов и агрегация ответвителей для финансовых рынков
Архитектура с нулевой потерей пакетов	•	•	—	•	—	•
Динамический компилятор фильтров	•	•	—	•	—	•
Высота системы (RU)	1	1	1	от коммутатора	1	1
Расширенная обработка пакетов	—	—	—	—	—	—
Проставление временных меток на входящем порту для последующей обработки	•	—	—	от коммутатора	—	—
АС резервный источник питания (горячая замена)	•	•	•	от коммутатора	•	•
DC резервный источник питания (горячая замена)	•	•	•	от коммутатора	•	•
Макс. пропускная способность обратной панели (Гбит/с)	720	480	12	от коммутатора	12	640
Макс. кол-во портов 1G	48	48	10	от коммутатора	26	64
Макс. кол-во портов 10G	72	48	4	от коммутатора	—	64
Макс. кол-во портов 25G	0	0	0	от коммутатора	—	0
Макс. кол-во портов 40G	18	0	0	от коммутатора	—	16
Макс. кол-во портов 50G	0	0	0	от коммутатора	—	0
Макс. кол-во портов 100G	0	0	0	от коммутатора	—	0
Макс. кол-во портов 400G	0	0	0	от коммутатора	0	0

	Перейти к Vision Edge 40	Перейти к Vision Edge 10S	Перейти к Vision Edge 1S	Перейти к Vision Edge OS	Перейти к Vision T1000	Перейти к TadeVision
Узнать больше						

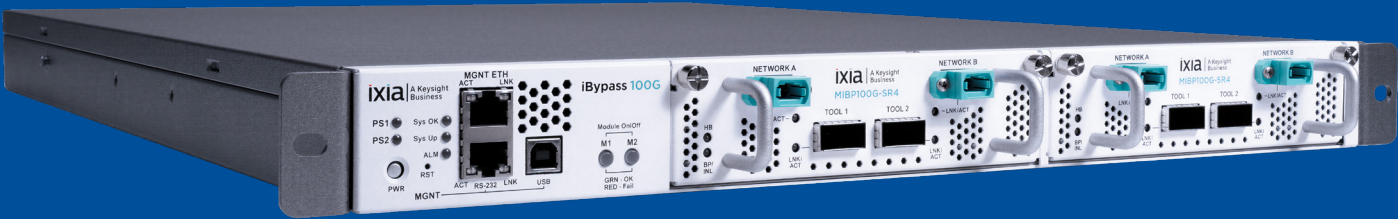
ОБХОДНЫЕ КОММУТАТОРЫ (BYPASS SWITCHES)



Узнать больше о том какой
обходной коммутатор
подходит для вашей сети:



Обеспечение времени безотказной работы и доступности сети



Внешние обходные коммутаторы являются ключом к высокой доступности и простоте обслуживания при развертывании сетевого мониторинга и систем безопасности. Хотя все признают необходимость таких инструментов, как системы предотвращения вторжений и межсетевые экраны, их встроенные модели развертывания могут создавать риск или простои, когда приходит время перезагрузки, технического обслуживания или замены. Внешние обходные коммутаторы, такие как Keysight iBypass, обеспечивают автоматическое переключение при отказе, которое предотвращает ситуации, когда обновления инструментов или простои выводят сеть из строя.

Keysight iBypass предлагает следующие ключевые функции:

- Поддержка резервной и последовательной архитектуры
- Высокая доступность: активный-активный или активный-резервный
- Предварительно настроенный сигнал контроля работоспособности (heartbeat)
- Централизованное управление
- Простой в использовании графический интерфейс пользователя (GUI)

Продукт	Описание	Тип среды	Сетей на устройство	Высокая доступность	Конфигурируемость	Обнаружение отказов линии
iBypass 100G	Односегментный интеллектуальный обходной коммутатор на 100G	100/40G	Оптика	1 или 2 сегмента	•	LFD
iBypass DUO	Обходной коммутатор высокой плотности с резервированным управлением	1G / 10G	Оптика	1 или 2 сегмента	•	LFD/LFDC
iBypass VHD	Обходной коммутатор очень высокой плотности, 12-сегментный интеллектуальный обходной коммутатор	1G / 10G	SFP+ / SFP	12 сегментов	•	LFD/LFDC
iBypass 4 Copper	Односегментный интеллектуальный обходной коммутатор для медных сетей	10/100/1G	Медь	1 сегмент	•	LFD/LFDC

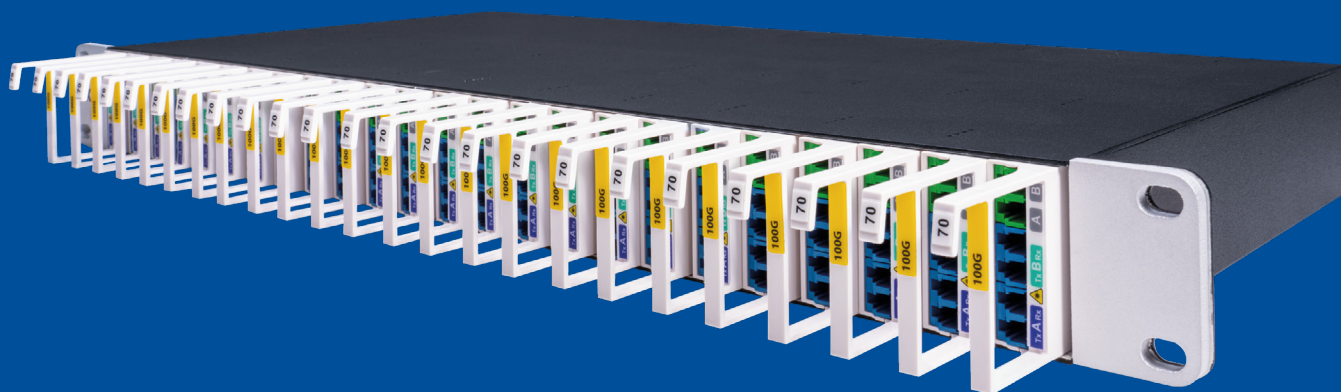
СЕТЕВЫЕ ОТВЕТВИТЕЛИ (NETWORK TAPS)



Узнать больше о том какой
сетевой ответвитель вам
подходит:



Основа динамической сетевой аналитики



Сетевые ответвители и обеспечиваемая ими чистая, нефиль-
трованная видимость сетевого трафика являются основой
динамической сетевой аналитики. В отличие от портов SPAN
или портового зеркалирования, ответвители обеспечивают
обзор всего трафика — включая некорректный трафик и ошибки,
которые обычно были бы отброшены. Такая истинная видимость
облегчает устранение неполадок, обеспечение безопасности
и проведение криминалистических исследований (форензики).

Keysight предлагает самый широкий выбор ответвителей для
любых сетей, включая оптические ответвители Flex Tap, ответ-
вители с усиленной безопасностью Flex Tap Secure+, медные
ответвители, агрегирующие ответвители и промышленные
прочные ответвители Tough Tap.

Ответвители Keysight предлагают следующие ключевые функции:

- Обеспечивают простоту «подключи и работай»
- Не требуют IP-адреса
- Обеспечивают невзламываемую безопасность
- Выпускаются в медном и оптоволоконном исполнении
- Поддерживают скорости до 400 Гбит/с



Продукт	Описание	Скорость	Тип порта	Особенности
Flex Tap	Модульные пассивные волоконно-оптические ответвители	1G до 400G	LC и MTP	• 40/100G BiDi PSM4, SR4, SR10 и QSFP+ 40G-LX4 • Несколько коэффициентов деления и типов волокон • OM3, OM4 и OS2
Flex Tap Secure +	Модульные пассивные волоконно-оптические ответвители с оптическим диодом	1G до 400G	LC	• Расширенная безопасность предотвращает случайную или преднамеренную инъекцию света или данных • Идеально подходит для законного перехвата, правительственных, военных и других развертываний с высокими требованиями безопасности
Patch Tap	Низколатентные пассивные волоконно-оптические ответвители	1G до 100G	LC	• Низкая задержка до < 8 нс • Нечувствительный к изгибам • Многомодовый OM4 • Одномодовый OS2
Copper Tap	Активные медные ответвители	10/10/1000 Mbps медь	RJ45	• Независимое автосогласование (подключайтесь к низкоскоростным сетям и отправляйте данные на высокоскоростные инструменты) • Физически разнесенные (воздушный зазор) мониторные порты — данные • Диод между инструментом и мониторными портами • Функция аварийного сквозного соединения (fail-to-wire)
Tap aggregators	Активные медные ответвители с режимом агрегации	10/10/1000 Mbps медь	RJ45	• Мониторинг полнодуплексного трафика с одной сетевой картой (NIC) • Агрегирует оба направления в одну мониторную линию связи • Работает как стандартный или агрегирующий ответвитель • Предлагает функцию аварийного сквозного соединения (fail-to-wire)
iLink Aggregator II	Несколько (x8) медных ответвителей с агрегацией. Также доступен в виде 16-портового SPAN-агрегатора. 16 входных портов 10/100/1G и 4 мониторных порта 10G SFP+ / любой-с-любым	10/10/1000 Mbps медь + 4x SFP+ для агрегации портов	RJ45/SFP	• Экономичный агрегатор ответвителей, предназначенный для объединения трафика с нескольких ответвителей • Поддерживает низкие и средние скорости, которые высокопроизводительные NPB часто не поддерживают • Встроенные ответвители имеют функцию аварийного сквозного соединения (fail-to-wire)

Прочные ответвители для промышленных сред



Разработанные с нуля, прочные ответвители Keysight являются первыми в отрасли усиленными сетевыми ответвителями, предназначенными для суровых условий эксплуатации. Они соответствуют расширенным температурным диапазонам, выдерживают удары и вибрацию и имеют оптимизированные медные и оптоволоконные порты 10/100, 1G и 10G. Прочные ответвители сертифицированы по стандартам Института инженеров электротехники и электроники (IEEE), включая IEEE 1613 для безопасности и IEC 61850 для протоколов связи интеллектуальных электрических устройств.

Медные прочные ответвители обеспечивают выносной (внеполосный) мониторинг для инструментов безопасности и производительности и дублируют все пакеты для полной видимости. Для дополнительной защиты времени безотказной

работы эти ответвители имеют резервные клеммные колодки разъемов питания. Если основной источник питания выходит из строя, ответвитель автоматически переключается на резервный источник питания. Если оба входных источника питания отказывают, ответвитель все равно будет пропускать трафик между своими сетевыми портами (размыкание при отказе).

Оптоволоконные прочные ответвители собирают и архивируют сетевой трафик. Оптимизированные для оптоволоконных сетей, работающих до отказа, со старыми и новыми типами волокон, встречающимися на удаленных подстанциях, эти ответвители соответствуют требованиям TAA. Вы можете развертывать их в любом встроенном соединении в сети.

Продукт	Описание	Скорость	Тип порта	Сертификация, стандарты и соответствие нормативным требованиям	Особенности
Copper Tough Taps Перейти на сайт: 	Промышленные активные медные ответвители	10/100/1000 Мбит/с медь	RJ45	TAA; IEC 61000-4-2,3,4,5,6,8,11; IEC 60068-2-6; IEEE-1613; UL 508 внесен в список; UL 60950-1; EN60950-1; CE; IEC 61850	- Поддерживает питание по Ethernet (PoE) - Автоматическое согласование скорости - Защищен конструктивно — без интерфейса управления и IP-адреса, он не освобождается от оков - Физически разнесенные (воздушный зазор) мониторные порты — диод данных между портами инструментов и отслеживаемыми портами предотвращает вредоносные инъекции из мониторинговой сети - Бесшумная работа - Монтаж на DIN-рейку - Без вентилятора - Диапазон рабочих температур от -40 С до +85 С
Flex Tough Taps Перейти на сайт: 	Промышленные многомодовые модульные пассивные волоконно-оптические ответвители	1G до 400G	LC	TAA; CE; RoHS 10	- Питание не требуется - Защищен конструктивно — без интерфейса управления и IP-адреса, он не освобождается от оков - Пропускает весь трафик (включая ошибки) со всех уровней - Компактный — 4 ответвителя в одном модуле - Полностью пассивное оптическое устройство - Модели OM1, OM5 с коэффициентом деления 70/30 - Развертывание в любом встроенном сетевом соединении - Монтаж на DIN-рейку - Тот же форм-фактор, что и у медного прочного ответвителя - Диапазон рабочих температур от -40 С до +85 С

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ВИДИМОСТЬЮ (KVO)



Узнать больше
о KVO:



Управление многими NPB через единую панель управления



Сети становятся все более сложными, как и задача извлечения из них информации о динамической сетевой аналитике. Инфраструктура видимости, состоящая из NPB, обходных коммутаторов и ответвителей, обеспечивает хорошую основу для вашей сети. Затем вам нужно управлять и координировать все эти системы. Именно здесь вступает в действие Keysight Visibility Central Management (Keysight Vision Orchestrator (KVO)).

Централизованное управление позволяет вам контролировать сотни устройств с помощью мониторинга, запланированных изменений конфигурации и массовых обновлений программного обеспечения. Вы можете импортировать или экспортировать конфигурации, запускать скрипты, просматривать использование пропускной способности и многое другое. Кроме того, вы можете настраивать панели мониторинга и интегрировать их с другими системами управления сетью через северные интерфейсы.

Централизованное управление Keysight предлагает следующие ключевые функции:

- Управление через единую панель управления
- Автоматическое обнаружение устройств
- Единый вход (single-sign-on) и автоматическая подготовка без вмешательства оператора (zero-touch provisioning)
- Физические или виртуальные форм-факторы
- Высокая доступность с плавающим основным / резервным IP
- Аутентификация RADIUS, TACACS+ и LDAP

ПЛАТФОРМА АКТИВНОГО МОНИТОРИНГА (НАWKEYE)

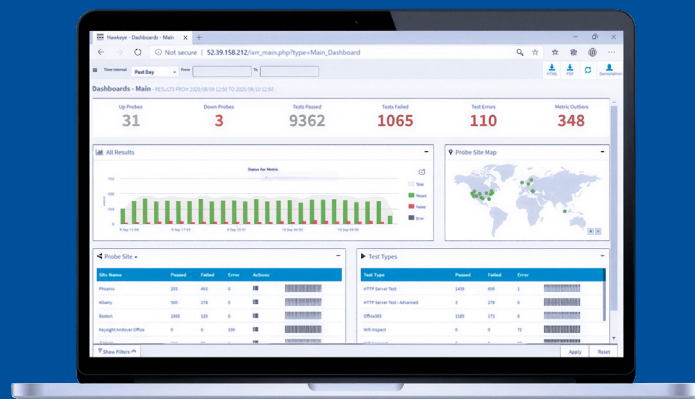


Узнать больше
о платформе:



Возьмите под контроль качество обслуживания пользователей с помощью активного/синтетического мониторинга производительности сети

Нawkeye
монитор консоли



Нawkeye
конечные узлы

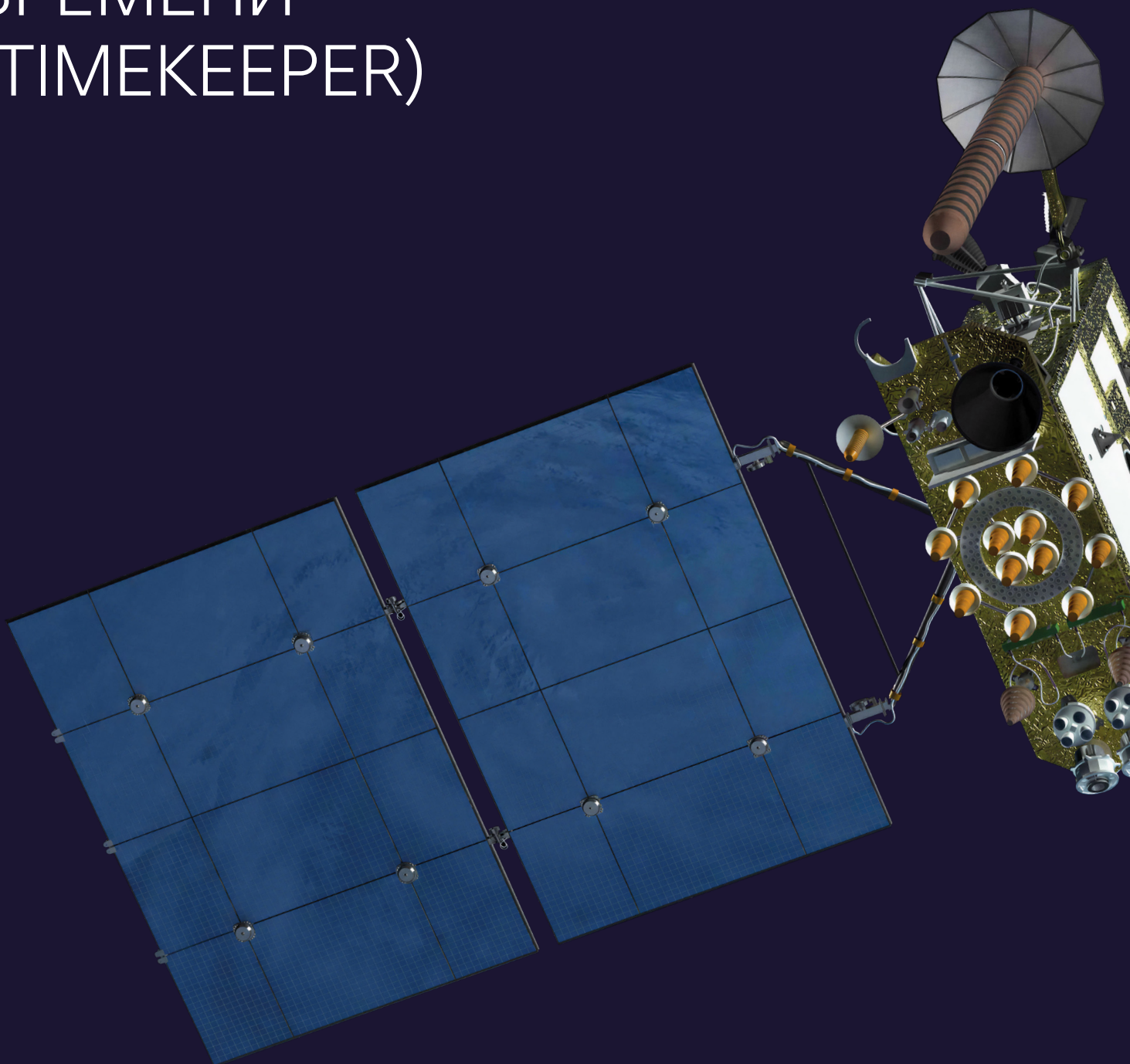
Будучи платформой активного мониторинга, Keysight Hawkeye помогает вам непрерывно управлять производительностью и связностью в вашей сети. Hawkeye упрощает мониторинг удаленных площадок, центров обработки данных, облачных сервисов и многого другого — все из одного инструмента.

Измеряете ли вы качество обслуживания удаленных пользователей через голосовые приложения, пользователей филиалов по Wi-Fi или общую связность с вашими приложениями «программное обеспечение как услуга» (SaaS) — легко контролировать, управлять и поддерживать пиковую производительность. С помощью Hawkeye вы можете делать все это и даже больше.

Нawkeye предлагает следующие ключевые функции:

- Надежная библиотека предопределенных тестов качества обслуживания
- Мониторинг голоса, видео и инструментов унифицированных коммуникаций с готовыми интеграциями
- Возможность просматривать все данные о производительности в одном интерфейсе и устанавливать пользовательские оповещения
- Мониторинг Wi-Fi 6 и проводных сетей
- Широкий выбор аппаратных платформ, таких как Vision 10S, XR3000, IxTap и IxProbe
- Скорости от 100 Мбит/с до 10 Гбит/с
- Версии программного обеспечения

СИНХРОНИЗАЦИЯ ВРЕМЕНИ (TIMEKEEPER)



Узнать больше
о TimeKeeper Server:



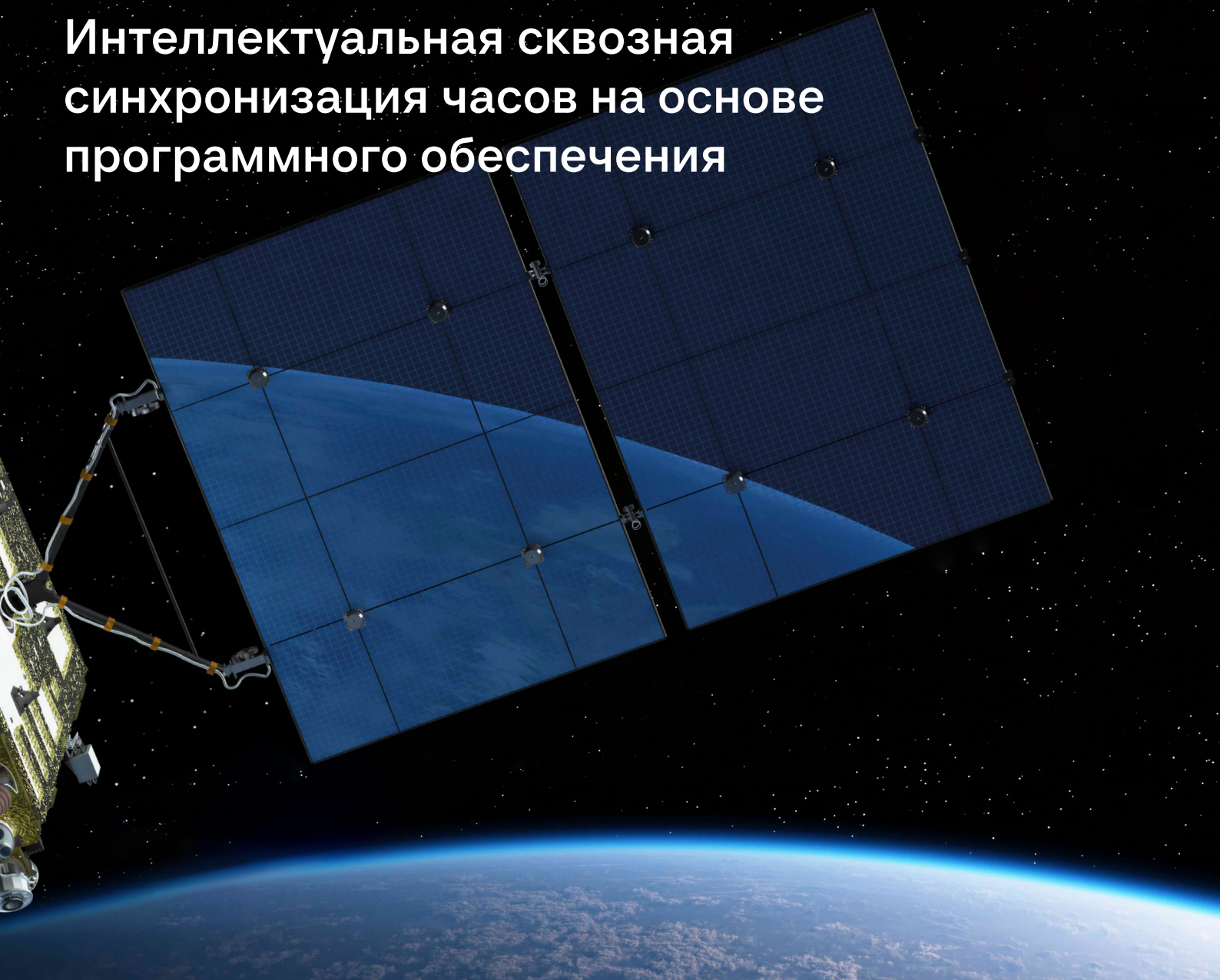
Узнать больше
о TimeKeeper Client:



Узнать больше
о TimeKeeper Compliance:



Интеллектуальная сквозная синхронизация часов на основе программного обеспечения



Из-за постоянно растущей зависимости от точного времени системы и процессы становятся все более уязвимыми для случайных или преднамеренных атак на временную инфраструктуру. Такие организации, как Агентство кибербезопасности и защиты инфраструктуры правительства США, настоятельно рекомендуют пользователям временных сервисов укреплять свою временную инфраструктуру и предпринимать шаги для обнаружения и реагирования на временные аномалии. Многие внутренние системы и процессы безопасности зависят от правильного и однозначного времени. Нарушение временных сигналов, таких как глобальная навигационная спутниковая система (GNSS), протокол сетевого времени (NTP) или протокол точного времени (PTP), может нарушить работу критически важных систем.

Программное обеспечение Keysight TimeKeeper, установленное на серверах, заменяет стандартные демоны времени. Оно позволяет предприятиям, поставщикам услуг и правительствам синхронизировать системные часы с несколькими источниками времени, доступными через публичный интернет или через временные сигналы GNSS, такие как GPS или Galileo. В дополнение к синхронизации, оно обнаруживает временные

аномалии и предупреждает о них. Более 100 финансовых учреждений и несколько правительств по всему миру установили TimeKeeper.

TimeKeeper предлагает следующие ключевые функции:

- Одновременная поддержка источников времени NTP и PTP
- Резервное переключение TrustedTime между несколькими источниками
- Полное оповещение и простые для понимания веб-графики временных ошибок
- Выбор между управлением через графический интерфейс пользователя (GUI) или командную строку (CLI)
- Опциональное долгосрочное отслеживание аудита для финансовых рынков
- Поддержка Linux или Windows Server
- Возможность предоставлять время и управлять сотнями клиентов с помощью TimeKeeper Server



ТЕЛЕФОН

+7 (495) 252-00-96

E-MAIL

INFO-SITE@AKMETRON.RU

САЙТ

WWW.AKMETRON.RU

СЕРВИСНЫЙ ЦЕНТР

SERVICE@AKMETRON.RU

АДРЕС

МОСКВА, УЛ. РАБОЧАЯ, Д. 93, СТР. 2,
М. «РИМСКАЯ», БЦ «НОВОРОГОЖСКИЙ»

Визитная карточка



Каталог

