Обзор решения IP Quality Monitor (IQM)

# Назначение IQM

IP Quality Monitor (IQM) — аппаратно-программный комплекс, предназначен для измерения, сбора и контроля значений качественных характеристик и параметров производительности на IP сетях.

Мониторингу может быть подвержена любая сетевая топология. В работе система учитывает ряд технических характеристик и абстрактных признаков: параметры передаваемого трафика, сетевые архитектурные уровни, сервисные уровни, зональную структуру, географию и т.д.

Измерения могут проводиться на различных уровнях сетевой модели OSI: канальном, сетевом, транспортном, сеансовом и прикладном.

Так же система может получать данные для мониторинга различными средствами от внешних источников: SNMP, CLI, HTTP, и т.д.

Для нестандартных методов система обеспечивает программируемые тесты. Любые абстрактные данные могут быть получены с программируемым тестом. Таким образом, элементы IQM могут работать в качестве адаптеров для получения данных и передачи их в базу для дальнейшего анализа, мониторинга, отображения.

# Состав IQM

Система состоит из агентов и ядра.

Агенты IQMA (IQM Agent) – аппаратно-программные средства, предназначенные для измерения качественных характеристик каналов связи. Измерения проводятся путем пропуска контрольного трафика с заданными параметрами через исследуемый сегмент сети. Для измерения характеристик на различных сетевых уровнях реализован ряд специализированных тестов.

Ядро IQMM (IQM Manager) выполняет следующие задачи:

* Управление подсистемами IQM,
* Конфигурация и контроль состояния агентов,
* Получение данных, их обработка и анализ,
* Сигнализация о нештатных состояниях,
* Представление собранной статистики в различных формах: графики, таблицы, отчеты, диаграммы,
* Предоставления доступа к персонализированным данным в личном кабинете,
* Административные функции.

# Подход к измерениям

На узлах сети размещаются специализированные аппаратно-программные комплексы агентов. Измерение качественных характеристик каналов связи осуществляется путем пропуска контрольного трафика с заданными параметрами через исследуемый сегмент сети между агентами. Использование проб на ключевых узлах сети позволит производить измерения не только сквозных параметров, но и на определенных ее участках, что облегчит в дальнейшем процесс локализации проблемы. Таким образом, например, можно осуществить мониторинг и управление качеством на одном из самых проблемных участков сети — на последних милях.



Агент-инициатор (т.е. агент, у которого хранится конфигурация теста) по заданным критериям определяет момент времени для запуска теста. Тест может запускаться:

* с заданной периодичностью, начиная с определенного момента,
* в определенные временным шаблоном моменты
* по расписанию

Инициатор устанавливает управляющее соединение с сопряженным агентом. Управляющая сессия авторизуется. После согласования параметров, для проведения измерений в каждом направлении, оба агента становятся источниками и приемниками тестового трафика. При пропуске тестового трафика, могут быть учтены различные параметры, определяющие профиль трафика и настраиваемые на различных уровнях от канального до прикладного.

# Параметры

Каждый из агентов фиксирует характеристики доставки в своем направлении. На сетевом/транспортном уровнях измеряются:

* Процент потерянных пакетов в каждом направлении,
* Круговые задержки,
* Односторонние задержки в каждом направлении,
* Вариация задержки (Jitter) в каждом направлении,
* Скорость, с которой был осуществлен прием тестовых пакетов в каждом направлении,
* Объем полученных тестовых данных,
* Процент пакетов доставленных с измененным классом сервиса,
* Процент пакетов доставленных с нарушением порядка.

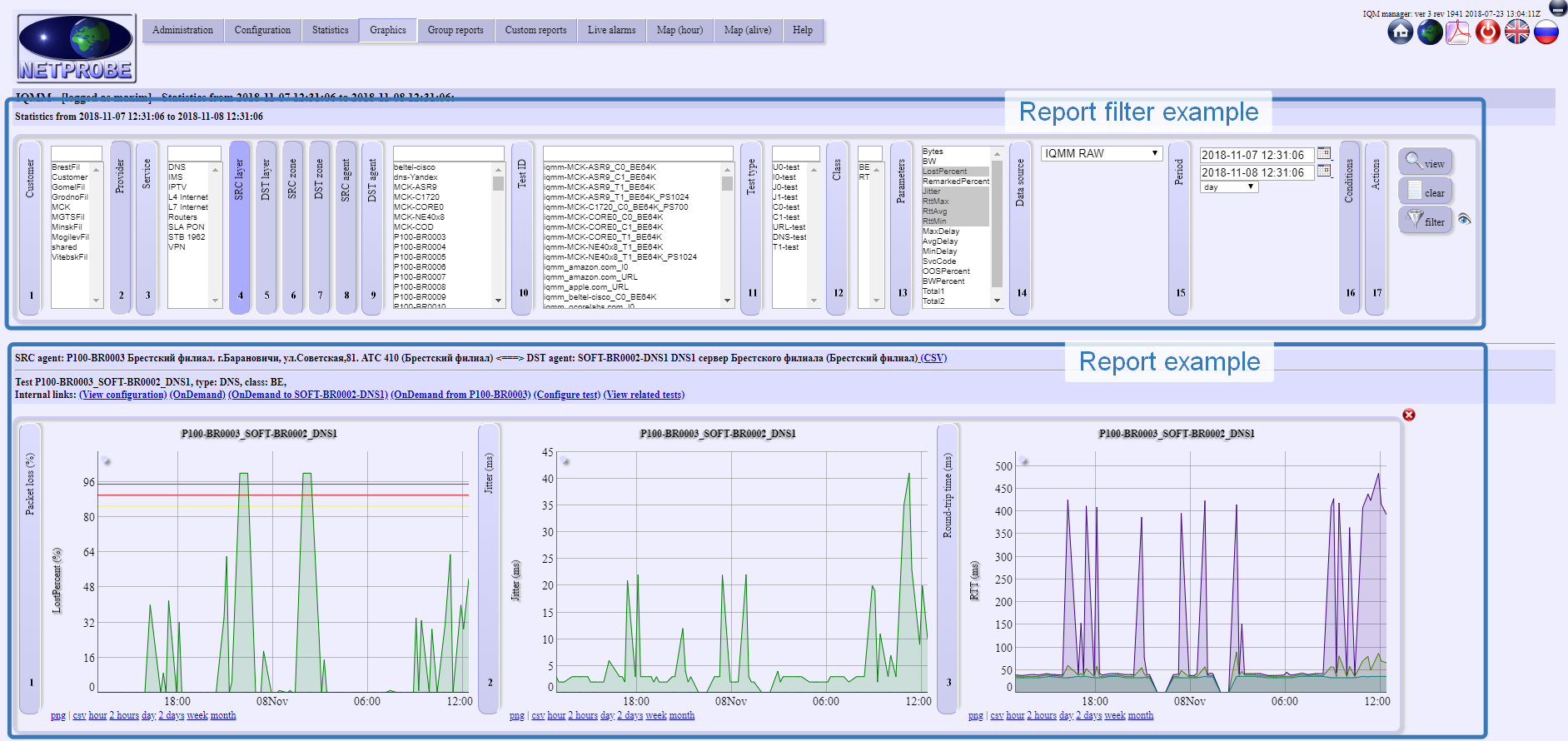
Измерение этих параметров может производиться в разных классах сервиса, например: standard, premium и real-time.

# Отображение и фильтрация данных

По окончании тестирования агент-инициатор получает от сопряженного агента измеренные характеристики, склеивает их со своими измерениями и записывает файл. С заданной частотой файл передается в систему управления. Обычно агент сам инициирует передачу своей статистики.

Полученные измерения обрабатываются и заносятся в базу данных. После этого данные подвергаются первичной обработке для обнаружения нарушений, проведения оповещения, агрегации. Система хранит три типа данных: сырые измерения и два типа агрегированных с часовым и суточным усреднением. Период усреднения возможно изменить.

После попадания данных в базу они становятся доступны для просмотра через интерфейс. Интерфейс предлагает различные средства визуализации данных: графики, таблицы, диаграммы, разнообразные отчеты. Функционал отчетов, определяемых пользователем, позволяет создавать собственные структуры отчетов. Отчеты экспортируемы в формат электронной таблицы. При формировании запросов предусмотрена возможность фильтрации запрашиваемых данных по различным признакам: клиентам, провайдерам, сервисам, сетевым архитектурным уровням, географическим зонам, агентам, тестам, классам сервиса, параметрам. Для осуществления фильтрации запрашиваемых данных предусмотрена возможность, как непосредственного выбора множества объектов из списка, так и возможность использования регулярных выражений, для автоматического выбора группы объектов.



# Политики контроля

Политики контроля действуют для произвольной группы измеряемых параметров, формируют несколько зон критичности и определяют способы реагирования на переходы между зонами критичности. Реагирование возможно как на единичные события, так и на события, возникающие чаще заданного порога. Предусмотрена возможность назначения каждому параметру нескольких пороговых значений: три пороговых значения, ограничивающих значение параметра сверху:

* Зеленый: предел нормального значения.
* Желтый: предел высокого значения.
* Красный: предел максимального значения.

и одно для ограничения снизу:

* Голубой: предел минимального значения.

При переходе параметра из одной зоны критичности в другую формируется событие, которое может быть связано с различными средствами оповещения:

* Уведомления средствами WEB-интерфейса
* e-Mail,
* SNMP-trap,
* syslog,
* механизм вызова внешних процедур позволяет реализовать любой желаемый способ уведомления: HTTP, SQL и пр…

# Поддержка сторонних агентов

Обеспечивается работа с агентами встроенными в функционал сетевого оборудования других производителей

* Cisco: IP SLA агент в строенный в функционал сетевой операционной системы IOS
* Juniper: RPM агент в строенный в функционал сетевой операционной системы JUNOS
* Accedian Networks. Проверено взаимодействие с пограничными устройствами линейки EtherNID и MetroNID
* Rad: Поддерживаются пограничные устройства Rad MiNID.
* Реализована возможность использования сетевых устройств средствами TWAMP (RFC5357)

При невозможности использования на удаленной стороне какого-либо специализированного агента, можно использовать любые сетевые устройства с запущенным сервисом UDP/ICMP-echo. Следует понимать, что все измерения при таком тестировании будут круговыми, однако, во многих случаях этого оказывается достаточно.

Агент может выступать в качестве инициатора теста, который будет проводиться между другими сетевыми устройствами. После завершения теста, агент может получать результаты проведенных измерений. Сам агент в тестировании не участвует. Этот подход позволяет проводить тестирование, не встраивая агента в адресное пространство контролируемой сети.

Например, с таким тестом, становится возможным выполнение команды VRF ping на маршрутизаторе, к которому осуществляется подключение удаленного сетевого устройства. В качестве примера можно упомянуть механизмы Cisco SNMP ping, Cisco CLI ping.

# Сервисы прикладного уровня

Для проведения тестирования на уровне приложения могут использоваться различные сетевые сервисы: FTP, HTTP, IMAP, RTSP, SMTP, TFTP.

При тестировании уровня приложений поддерживаются следующие возможности:

* использования протокола SSL (Secure Sockets Layer – уровень защищённых сокетов) на уровне представления модели OSI. Таким образом, поддерживаются защищенные протоколы HTTPS, FTPS и другие.
* Проведение серии взаимодействий в рамках одного транспортного соединения позволяет повлиять на механизм TCP-window и осуществить разгон TCP-сессии.
* Раскраска трафика в заданный класс сервиса,
* Авторизация доступа к сервису
* При тестировании HTTP сервиса поддерживаются:
  + cookies,
  + HTTP-redirects,
  + режим HTTP persistent connection, также называемый HTTP keep-alive, или повторное использование соединений HTTP — использование одного TCP соединения для отправки и получения множественных HTTP запросов и ответов вместо открытия нового соединения для каждой пары запрос-ответ.

Функциональность интерпретатора тестов (пакетного теста) позволяет пользователю создавать любые тесты, реализовать произвольную логику тестирования любого сервиса, проводить любые измерения либо сбор рабочих параметров с сетевых устройств.

# Пропускная способность

Задача измерения пропускной способности распадается на две подзадачи: измерения емкости, доступной для тестового трафика и измерения текущей утилизации канальной емкости.

Как правило, не требуется регулярного подтверждения возможности предоставленного канала по пропуску трафика на контрактной скорости. Это, обычно разовая задача, которая возникает на этапе сдачи-приемки канала в эксплуатацию, либо при обоснованном подозрении о несоответствии возможностей канала заявленной скорости. В таких случаях возможно проведение тестирования пропускной способности канала с его полной загрузкой тестовым трафиком. Если все же присутствует потребность в регулярном тестировании, можно воспользоваться временными шаблонами для проведения тестов в ночные часы или во время, когда канал не нагружен. Так же, тестирование можно запустить по требованию, после предварительного согласования нагрузки.

Если на сети поддерживаются классы сервиса, а любой сервисный трафик обслуживается с бОльшим приоритетом, чем неприоритетный Best-Effort, то возможно проведение тестирования с неполной нагрузкой. Например, 20% загрузка канала тестовым трафиком в классе Best-Effort позволит выявить момент, когда тестовый трафик начнет вытесняться сервисным.

Так же, система IQM поддерживает интеллектуальное измерение пропускной способности путем разгона тестовой сессии до достижения заданного уровня потерь в канале.

Все же, в большинстве случаев, требуется контроль занятой полосы. Система IQM предусматривает средства контроля утилизации канальных емкостей. Для этого система укомплектована SNMP-коллектором.

# Мониторинг IPTV

Система IQM предлагает решение для контроля качества поставщиков услуг IPTV и работы головных станций (Headends). Для этого реализован отдельный модуль MReceiver, инициируемый агентом измерений IQMA. Модуль осуществляет подписку на мультикаст-видео, принимает и анализирует пакеты потока MPEG-TS. На данный момент поддерживается метод вещания: MPEG-TS поверх UDP. Измеряются характеристики доставки видео согласно методикам RFC 4445 – A Proposed Media Delivery Index (MDI), а так же дополнительные характеристики. Результаты измерений передаются менеджеру IQM, где они могут быть проанализированы политиками контроля и представлены операторам наряду с другими измерениями. Измеряются параметры:

* **Delay Factor, DF (ms)**: В RFC4445 определяется как абсолютная разница между объемом данных пришедших в буфер из сети и объемом данных, забираемых из буфера для непрерывного воспроизведения, деленная на битрейт. Измеряются минимальные, средние и максимальные значения DF за сессию.
* **Media Loss Rate, MLR (pps)**: MLR – количество потерянных или пришедших в неправильном порядке пакетов в секунду. Рассчитывается как отношение разности количества ожидаемых пакетов и количества принятых пакетов к интервалу времени (RFC4445). Сохраняются максимальные и средние за период измерений значения.
* **Media Loss Packets, MLP (p)**: количество MPEG-TS пакетов, поступивших с нарушением CC.
* **Media Loss Bytes, MLB (B)**: количество байт MPEG-TS пакетов, поступивших с нарушением CC.
* **Media Loss Time, MLT (ms)**: количество миллисекунд, в течение которых были зафиксированы потери MLR.
* **Bitrate (bps)**: общий объем пакетов в битах MPEG-TS принимаемых в единицу времени.
* **NumPacketsTS (p)**: количество MPEG-TS пакетов полученных ресивером после распознавания и регистрации потока
* **Join Time (ms)**: Время прошедшее с момента подписки на поток до получения первого пакета в потоке MPEG-TS.
* **Inter-packet Arrival Time, IAT (ms)**: интервал в миллисекундах между приходом двух последовательных UDP-пакетов транспортного потока. Сохраняются среднее и максимальное за период измерения.

# Аппаратные решения IQMA

В зависимости от потребностей заказчика IQM агент может поставляться в виде программного обеспечения или аппаратно-программного комплекса.

При поставке в виде АПК, в качестве аппаратной платформой могут выступать различные платформы. Наиболее распространенные варианты:

## 100Mbps агент

Агент на базе AK-systems IP Plug (IQMA-P100). Является наиболее распространенным решением клиентского уровня. Агент разработан и произведен в РФ специально под задачу измерения характеристик доставки сетевого трафика. Поддерживается 802.1q VLAN, опционально возможна установка WiFi-модуля и USB порта.



Микропроцессор: ARM 1ГГц   
Память: до 1024Мб 16 бит DDR2@800 МГц, до 4 ГБ NAND Flash

Ethernet: Gigabit Ethernet

Питание: 100 – 240 В, 50/60 Гц; потребляемая мощность: 15 Вт, 5В@3,0А max

Габариты: 118мм(Д) х 76мм(Ш) х 43мм(В)

Аналогичная платформа предназначенная для монтажа в стойку (IQMA-R100):



## 1 Gbps агенты

Агент на базе Small Form-Factor Micro-ITX PC (75х225х315mm):



Агент для монтажа в стойку (IQMA-R1000):



Агент IQMA-R1000 является наиболее распространенным решением уровня концентрации. Агент разработан и произведен в РФ специально под задачу измерения характеристик доставки сетевого трафика. Поддерживается 802.1q VLAN.

## 10 Gbps агенты

На базе платформы российской компании AK-Системс (Комплаг) подготовлена платформа 10 гигабитного агента (Для заказа: IQMA-R10G). Платформа позволяет произвести тестирование на скорости физического интерфейса.

Агент оснащен двумя портами 10 Gigabit Ethernet. Возможен заказ агента с оптическими интерфейсами.



## 100 Mbps агент на базе решений GlobalScale

ПО IQM агента для ARM. На текущий момент поддерживается для различных микрокомпьютеров производимых компанией GlobalScale. Среди них SheevaPlug, DreamPlug, MiraBox, GuruPlug.



## Агенты на базе сетевых устройств

Агенты могут работать на различных платформах, неполный перечень которых приводим далее:

* ПО IQM агента для NSG маршрутизаторов (широко распространенных в платежных терминалах и банкоматах).

Агент на базе маршрутизатора NSG-700:



Для широкого спектра embedded-устройств на базе ОС Linux доступна опция респондера IQM агента. Респондер позволяет проводить сессии измерения качественных параметров, инициируемые IQM-агентом. Опция респондера предъявляет минимальные требования к памяти и была разработана специально для систем с ограниченным количеством памяти.

На текущий момент поддерживаются работа респондера IQM агента на маршрутизаторах RouterBoard компании Microtik:



на линейке компактных встраиваемых компьютеров, производства компании Moxa:



# Интеграция с внешними системами

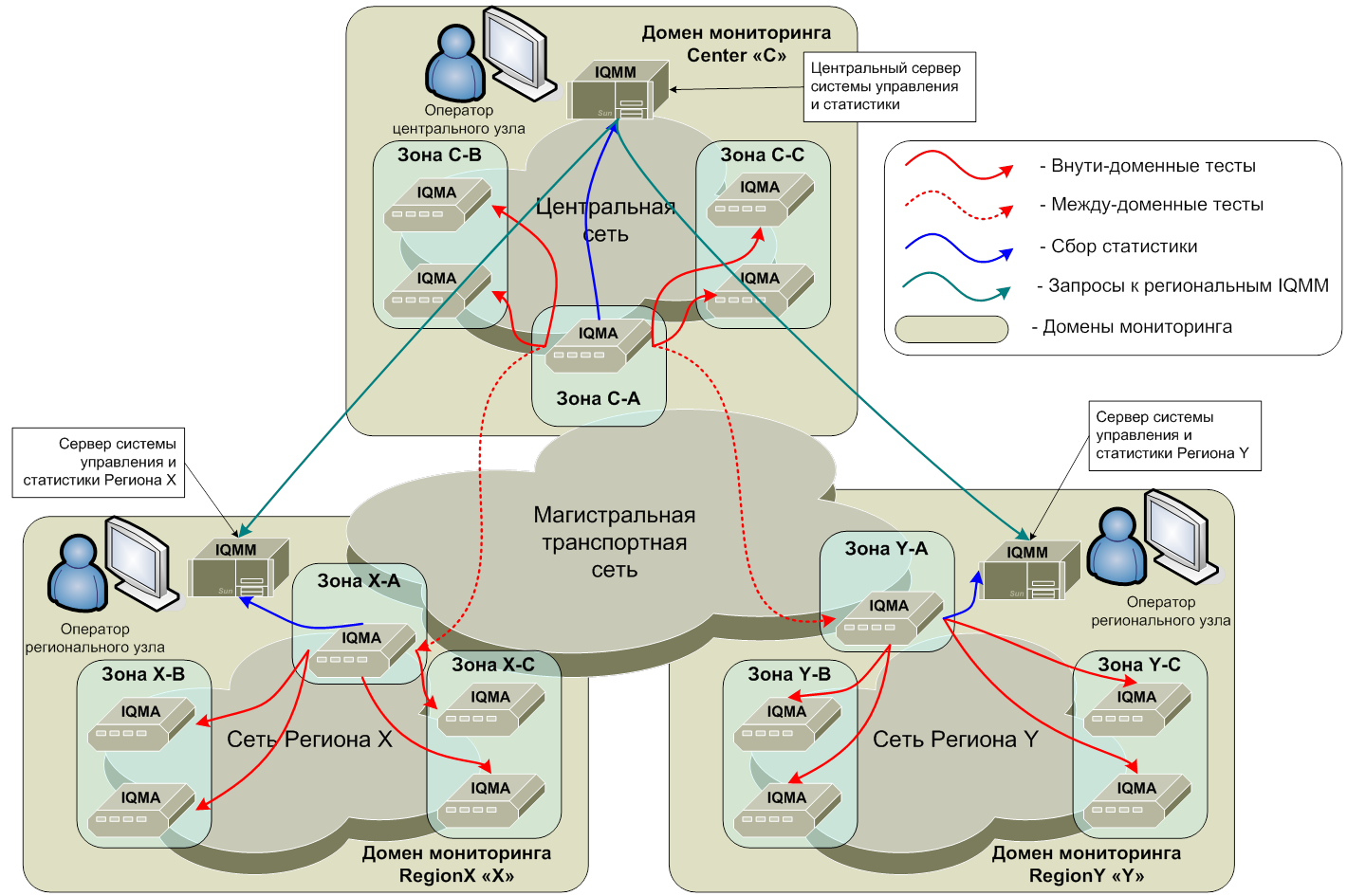
Возможна интеграция с внешними системами мониторинга через стандартные интерфейсы. Для этого предлагаются следующие средства:

* На уровне уведомления об обнаруженных нарушениях предлагаются стандартные интерфейсы: syslog, SNMP-trap, e-Mail, HTTP, SMPP…
* Для интеграции на уровне интерфейса реализована JavaScript библиотека, позволяющая встраивать любые элементы интерфейса в HTML-страницы.
* Для управления потребуется IQM-driver. Он реализует упрощенный интерфейс для автоматизации работы с агентами, тестами, другими объектами менеджера. Возможна работа в двух режимах: обращение к драйверу со стороны внешней системы через WEB или через CLI. Возможно так же комбинирование этих средств. Драйвер может работать как на одной аппаратной платформе с системой управления IQMM, так и на выделенной.

# Распределенный мониторинг

Система IQM позволяет реализовать распределенный мониторинг качественных параметров IP сети.

Контролируемая сеть может иметь ярко выраженную территориально распределенную структуру, с несколькими центрами концентрации трафика, региональными сетями. В этом случае разумным решением будет разбить сеть на домены мониторинга. Каждый домен будет представлять собой полноценную систему мониторинга с агентами и системой управления. Все региональные домены будут подчиняться центральной системе управления.



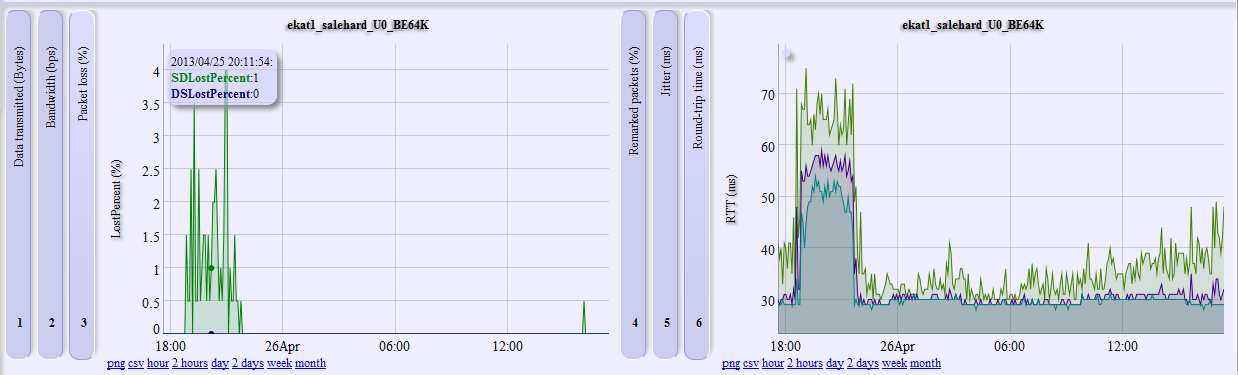
На рисунке изображен пример построения распределенной системы мониторинга. Региональные операторы используют собственные региональные системы управления для контроля и управления своими агентами. При необходимости, права управления можно перенести в центр, оставив региональным операторам права на просмотр. В этой схеме, информация о проведенных тестах не уходит дальше домена мониторинга. Центральная система управления имеет доступ к статистике всех доменов через региональные системы.

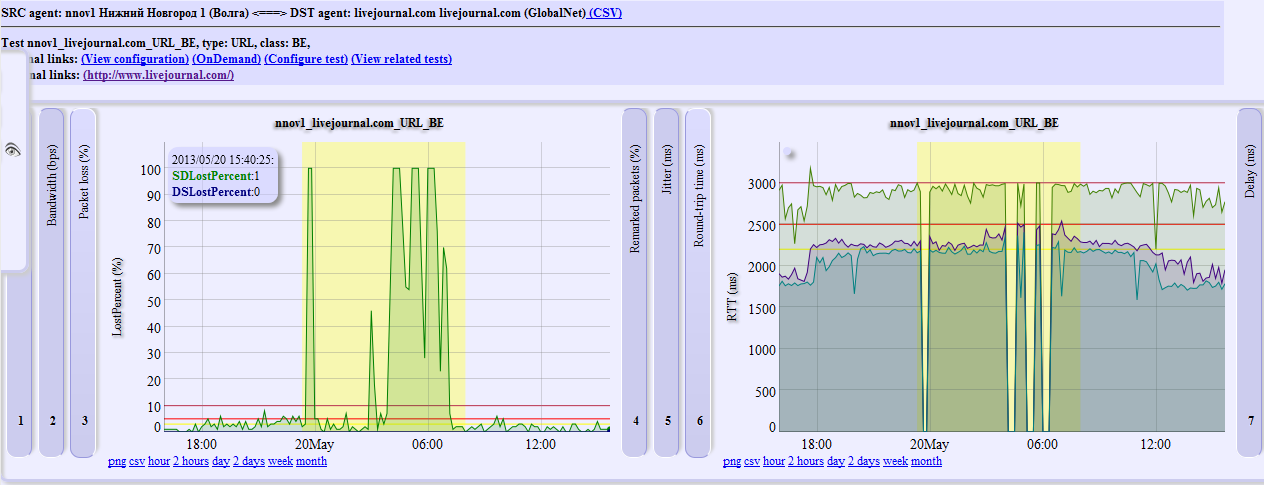
# Экранные формы

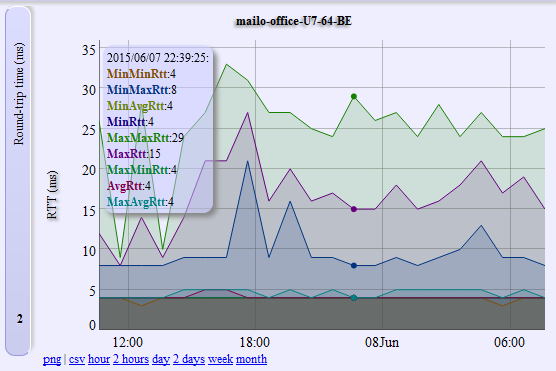
NB: Интерфейс поддерживает Русский и Английский языки, возможна локализация для любого другого языка.

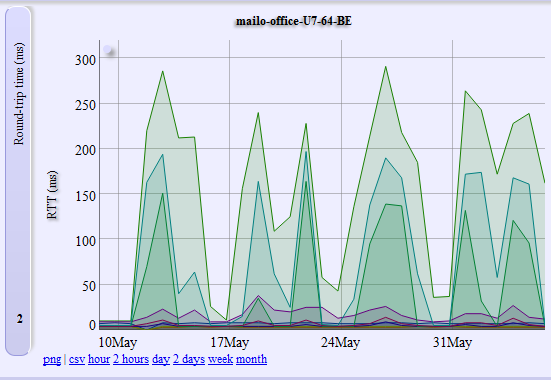
## Графические отчеты

На графиках представлены результаты DDOS-атак на сайт Livejournal, на примере видно, что сервис был недоступен для клиентов Нижнего Новгорода и Екатеринбурга.



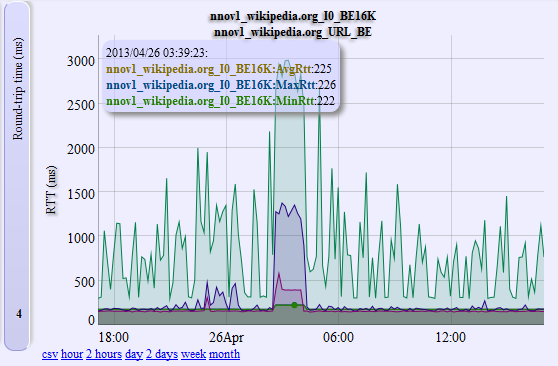
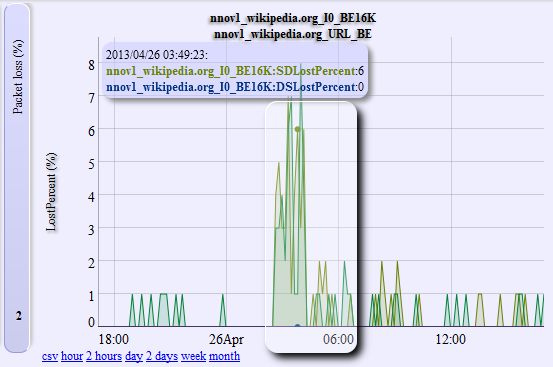




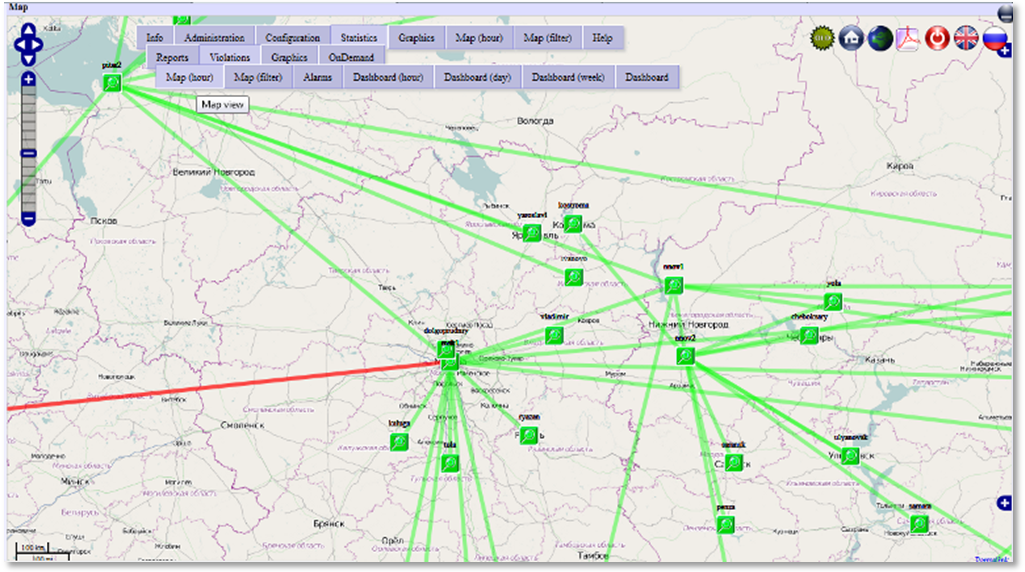


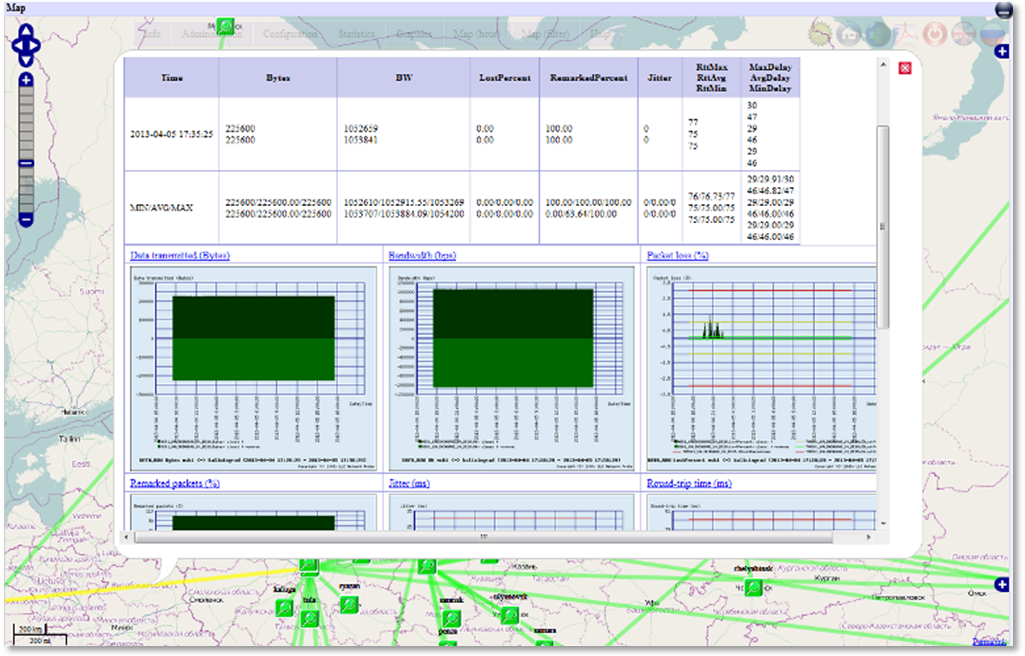
## Комбинированные отчеты

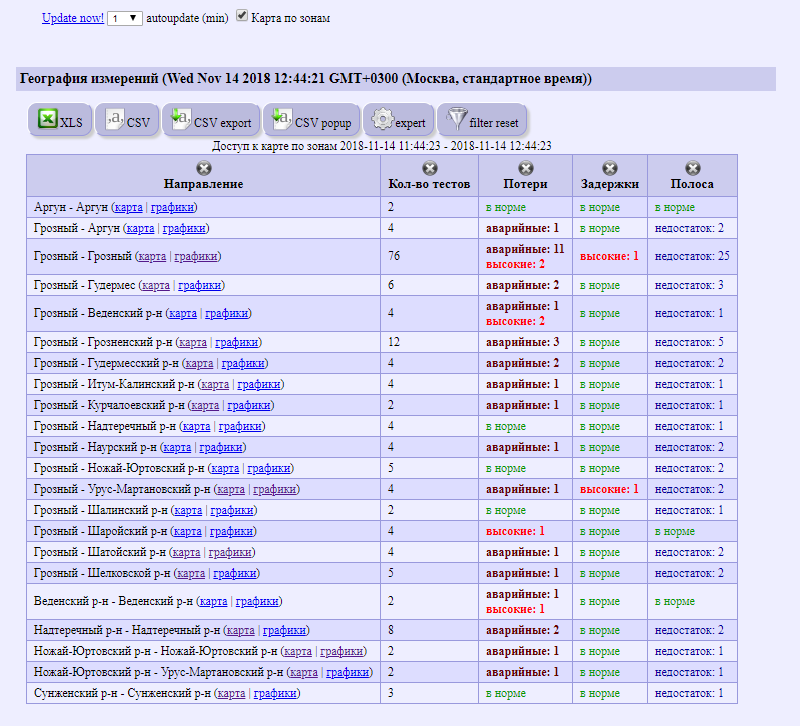
Для облегчения анализа измеренных агентами качественных характеристик есть возможность комбинирования отчетов. Приведено наложение данных, измеренных тестами, производимых на транспортном и на прикладном уровнях. На графиках видно, что недоступность HTTP сервиса была вызвана потерями на транспортном уровне, а минимальный порог задержки получения страницы с сайта wikipedia определяется возможностями транспортной среды.



## Гео-мониторинг

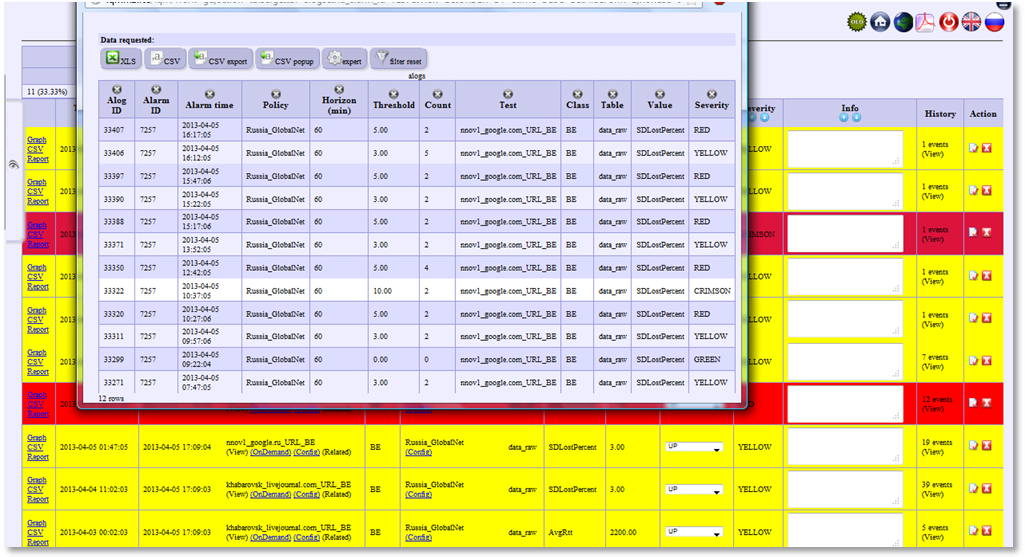


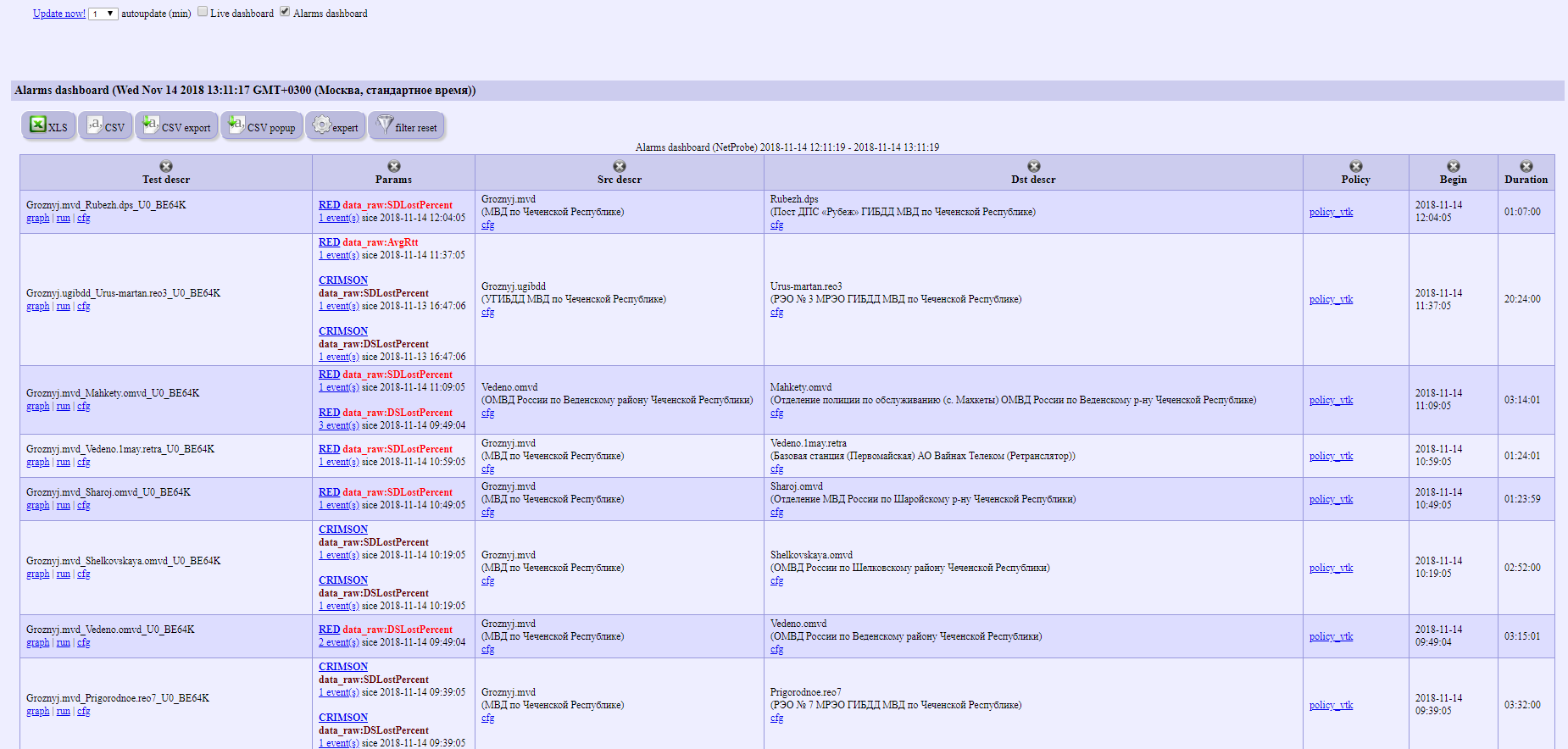




## Аварийные сообщения

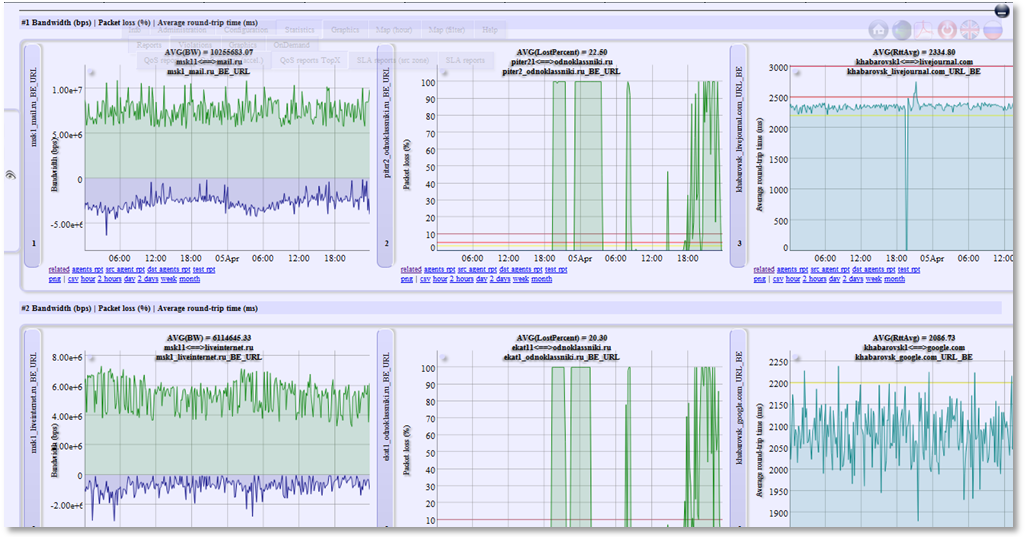
Поток аварийных сообщений с историей по отдельному объекту и табло алармов на базе пользовательского отчета





## TopX отчеты

Пример отчета с TopX, на основе L7 тестов: лидеры с максимальной скоростью загрузки страниц, с максимальным количеством потерь, с максимальной задержкой. Наивысшая скорость отдачи по HTTP у mail.ru, в лидеры по потерям попали одноклассники, сайт которых был не доступен по техническим причинам, наибольшие задержки от ЖЖ до Хабаровска.



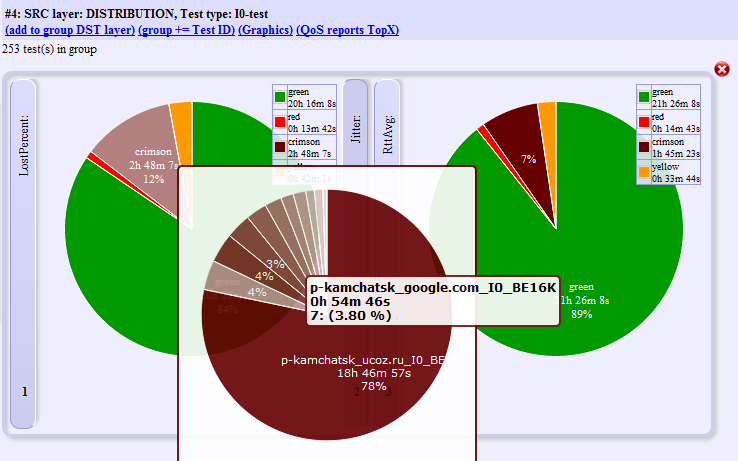
## Отчеты по параметрам

Информация в табличном виде о минимальных, средних и максимальных значениях контролируемых параметров за заданный отчетный период.



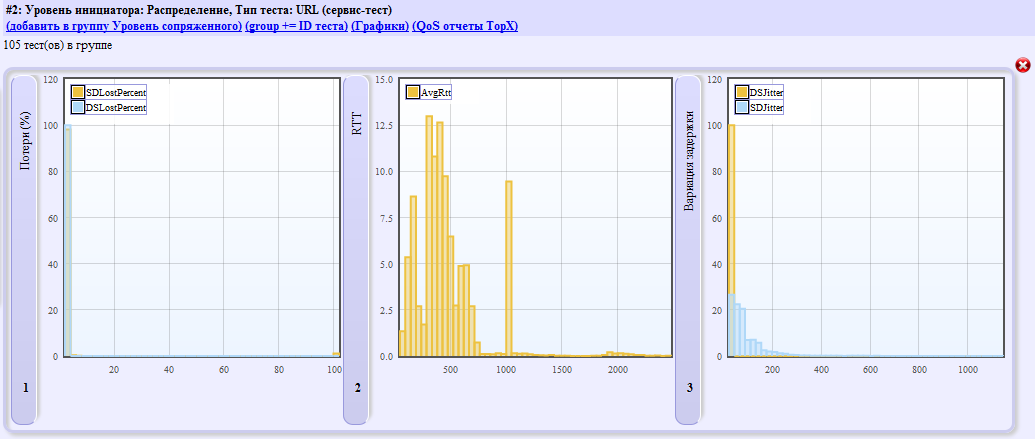
## Групповые отчеты по нарушениям

Пример отчета по распределению нарушений между тестами определенного типа:



## Групповые отчеты по распределению значений

Пример отчета по распределению значений между тестами определенного типа:



## Отчеты доступности

