Испытание концепции

Версия: 1.3 // 21.07.2016 18:15

Решение виртуализации сетевых функций на платформе RAD

RAD Data Communications Ltd. http://www.rad.com
International Headquarters: 24 Raoul Wallenberg Street, Tel Aviv 69719, Israel
Tel: +972 (3) 645-8181 **Fax:** +972 (3) 649-8250 **Email:** market@rad.com
Представительство в России: 115191, Москва, ул. Большая Тульская, д. 10, стр. 9, эт. 7, оф. 9506
Тел.: +7 (495) 231-1239 Email: info_russia@rad.ru
http://www.rad.ru/3-12218/Contact-us/

Содержание

1. Введение

Данный документ описывает подтверждение концепции решения RAD по виртуализации сетевого функционала на основе платформы ETX-2i с применением виртуализованных функций отечественного производства.

Для испытаний по подтверждению концепции была выбрана схема из двух соединенных через коммутатор демаркационных устройств с поддержкой платформы виртуализации, на которых последовательно развернуты и настроены виртуальные машины со следующими виртуальными функциями отечественной разработки:

- IP-АТС, разработки НТЦ ПРОТЕЙ
- VPN шлюз и межсетевой экран, разработки ОАО «ИнфоТеКС»

Само решение RAD представляет собой программно-аппаратный комплекс, состоящий из:

- Демаркационных устройств ETX-2i с поддержкой x86 платформы для виртуализации сетевых функций
- Системы оркестрации RADview, которая осуществляет автоматизированное управление устройствами RAD, а также предоставляет полноценный набор инструментов FCAPS для диагностики и контроля состояния сети

Приведенные в данном отчете испытания осуществлялись на территории компании RAD Data Communications LTS в лабораторных условиях.

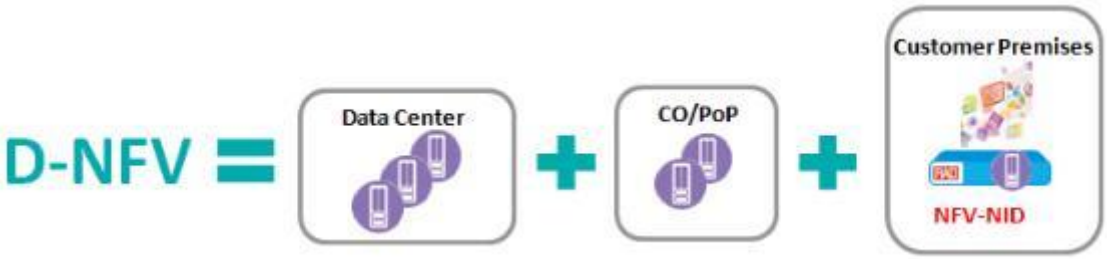
2. Описание решения и составляющих элементов

Виртуализация сетевых функций (NFV – Network Functions Virtualization) – это технология, при которой специализированные сетевые устройства заменяются на программное обеспечение, работающее на процессорах общего назначения. Наиболее популярное применение NFV в настоящий момент – центры обработки данных. Операторы связи также проявляют интерес к преимуществам, которые дает NFV, такие как:

- Ускоренное внедрение услуг для бизнес- и потребительского сектора и быстрая прибыль
- Новый сетевой функционал, соответствующий изменяющимся потребностям рынка
- Снижение расходов за счет применения готовых серверов (COTS)

Особый подход RAD подразумевает распределенный функционал **NFV - D-NFV (Distributed NFV)**, когда виртуализация сетевых функций (VNF) возможна по всей сети, в тех местах, где она наиболее эффективна и экономически оправдана. Виртуализация может осуществляться в ЦОД, в сетевых узлах и на площадке заказчика. В некоторых случаях эффективной является именно виртуализация на площадке заказчика, например, когда требуется разместить функционал как можно ближе к конечному пользователю. Это справедливо для защитных экранов, средств диагностики, IP-PBX, акселерации трафика, преобразования сетевых адресов и ограничения скорости. Универсальный оркестратор D-NFV управляет всей инфраструктурой VNF и виртуальных машин (VM), где бы они не находились, и применяет механизмы, схожие с SDN, для оптимизации размещения виртуальных функций.

RAD предлагает реализацию D-NFV с помощью новаторского решения, включающего платформу x86 для хостинга виртуального сетевого устройства L2/L3 NID, управляемого оператором связи. Это решение позволяет управлять обычными сетевыми устройствами, виртуальными сетевыми функциями и ИТ-приложениями, используя принципы SDN.



Размещение сетевого функционала на площадке заказчика может быть обусловлено следующими причинами:

- Некоторые функции должны оставаться на площадке заказчика: кольцевые проверки, сквозная защита, ограничение трафика, шифрование, оптимизация WAN
- Некоторые функции лучше работают на площадке заказчика: сквозной контроль качества QoS, мониторинг потребительского качества QoE приложений
- Качество некоторых функций может деградировать из-за ограничений сети: пропускной способности, задержек, доступности
- Ускоренное обслуживание заказчика с последовательным соединением приложений
- Требования высокой производительности и надежности работы центров обработки данных могут приводить к неоправданным затратам
- Большая гибкость инвестиций при внедрении сетевого функционала: D-NFV позволяет в пилотном режиме опробовать новые сетевые функции, повсеместно внедряя только те, которые окажутся успешными. Таким образом инвестиции основываются на результативности
- Снижение затрат за счет интеграции различных функционалов и приложений в одном устройстве
- Некоторые функции должны оставаться близко к заказчику в силу корпоративных правил безопасности, авторизации доступа и privacy

Платформа виртуализации ETX-2i

Демаркационные устройства Carrier Ethernet ETX-2i позволяют оператору связи предоставлять Ethernet услуги с SLA до площадки абонента по любой технологии доступа (GbE, 10GE, PDH, SHDSL). Устройство способно обрабатывать до 8 Гб/с пользовательского трафика с учетом политик управления трафиком и QoS, позволяя тем самым операторам предлагать несколько услуг на одном физическом порту.

ETX-2i имеет надежность 99.999% и предоставляет возможность сквозного контроля качества канала («end-to-end»). Как часть портфолио EtherAccess, ETX-2i идеально подходит для операторов фиксированных и мобильных сетей для предоставления услуг связи B2B/B2G/B2O.

Все эти модели семейства ETX-ETX-2i построены на единой программной платформе и имеют одинаковый программный функционал. Краткие особенности устройств:

- Унифицированное демаркационное устройство для передачи услуг L2/L3 VPN и TDM
- Возможность подключения абонента по любой технологии доступа: GbE/10GE Ethernet, PDH/SDH, SHDSL
- Оборудование операторского класса, поддерживающее линейное резервирование (G.8031, Dual Homing), кольцевую топологию (G.8032)

Рисунок 1: Обзорный вид устройств ETX-2i

- Позволяет осуществить переподписку канала за счет интеллектуального механизма управления полосой пропускания (CIR/EIR)
- Обработка многоприоритетного потока данных с контролем качественных характеристик: задержек, их вариаций, потерь пакетов, доступности услуги связи и объема передаваемого трафика
- Контроль качества L2/L3 сетей с помощью протоколов OAM (IEEE 802.1ag / ITU-T Y.1731) и TWAMP (RFC-5357), реализованный на аппаратном уровне
- Проведение нагрузочных тестов RFC-2544/Y.1564
- Расширенные опции по синхронизации: Synchronous Ethernet, 1588v2 Slave, BC, TC и Grandmaster
- Опция с поддержкой виртуализации сетевых функций

Система оркестрации RADview

Рисунок 2: Скриншоты системы управления и контроля качества услуг связи и оркестрации RADview

RADview – это комплексная система сетевого управления, состоящая из следующих модулей:

- RADview Element Management System – система автоматизации и управления элементами сети
- RADview Service Manager – система автоматизации и управления услугами связи
- RADview Performance Monitoring – система контроля качества услуг связи
- RADview Orchestator – система оркестрации и управления решением D-NFV

Система оркестрации RADview D-NFV Orchestrator использует платформу OpenStack для управления физическими и виртуальными ресурсами, выделенными для работы решения D-NFV и использующимися для быстрого развертывания дополнительных услуг связи на периметре абонента. Система разворачивает, настраивает и контролирует виртуальные машины на x86 D-NFV модуле, установленном в оборудовании RAD. В добавление к этому, в оркестраторе хранится репозиторий виртуальных функций, одобренных и сертифицированных компанией RAD для оптимальной работы, из которого осуществляется загрузка функций на устройства. Используя интуитивно понятный графический интерфейс в виде WEB-портала, система позволяет осуществить разворачивание и конфигурацию сервисов с применением виртуальных функций в несколько простых шагов, а также контролировать состояние и рабочие характеристики модуля x86 D-NFV.

Краткие особенности системы оркестрации RADview:

- Конфигурация и мониторинг с помощью открытой платформы OpenStack
- Хранение репозитория функций с полной информацией о производителе, использовании и системных требованиях
- Загрузка и настройка (провиженинг) множества сетевых функций на D-NFV модуль
- Инвентаризация модулей x86 и контроль их использования
- Развертывание программной оболочки модулей DNFV-OS, осуществление обновлений ПО
- Веб-клиент с интуитивно-понятным графическим интерфейсом

Краткие особенности системы RADview:

- Система управления элементами сети на платформе PC на основе SNMP
- Функциональные возможности управления элементами в соответствии с рекомендациями TMN
- Интегрируется с SNMPc Castle Rock
- Поддержка иерархических структур сети и многоуровневых карт
- графическое представление статистики, тенденций и показателей работы сети в реальном времени
- Часть системы сетевого менеджмента RADview
- Хранение и наглядное представление KPI, собранных от оборудования RAD
- Управление установкой пороговых значений
- Генерация отчетов
- Обнаружение деградации сервисов
- Управление и администрирование платформ виртуализации RAD D-NFV
- Провиженинг сервисов с виртуализированными функциями

Виртуальная функция: ПРОТЕЙ mCore.MKD (vPBX)

Виртуальная PBX – это учрежденческо-производственная АТС (УПАТС).

RAD ETX-2i на базе платформы виртуализации позволяет создавать несколько одновременно работающих виртуальных PBX (vPBX). Каждая vPBX – это полноценный коммутатор с собственным набором управляющих данных.

Оператор связи, используя данную возможность, может вести гибкую политику развития своей сети связи, одновременно уменьшая накладные расходы при ее эксплуатации.

mCore.MKD на основе единой аппаратно-программной платформы обеспечивает следующие функциональные возможности:

- Управление вызовами и маршрутизация. Коммутатор выполняет поиск направления вызова и предоставляет вызывающей стороне информацию о точках соединения, используя которую оборудование вызывающего и вызываемого абонентов будет способно установить соединение.

- Поддержка базовых абонентских услуг и широкого набора дополнительных услуг (переадресация, постановка на ожидание и другие), включая контроль доступа абонентов к местной/междугородной/международной телефонной связи.
- Совместимость с оборудованием сторонних производителей. Для взаимодействия с внешними устройствами используются стандартные аппаратные средства, имеющиеся на каждом сервере. Кроме того, используются стандартные программные протоколы. Все это дает возможность использования совместно с mCore.MKD не только оборудования производства компании ООО «НТЦ ПРОТЕЙ», но и оборудования сторонних производителей.
- Легкость в эксплуатации. mCore.MKD - это программный продукт, работающий на универсальных серверах и не требующий специфичного оборудования поддержки. Поэтому такие параметры, как габаритные размеры, вес, потребление, зависят от конкретной аппаратной платформы, на которой установлено ПО mCore.MKD.
- Программное обеспечение mCore.MKD работает под управлением операционной системы Linux.

mCore.MKD обладает следующими характеристиками:

- простота управления и наращивания производительности;
- поддержка оборудования, использующего различные протоколы сигнализации;
- гибкость управления концентрацией и маршрутизацией (интеллектуальная маршрутизация);
- выполнение задач авторизации и биллинга вызовов в пределах mCore.MKD;
- сокрытие структуры собственной сети или сети партнеров, если это необходимо;
- поддержка развитого набора дополнительных услуг;
- опциональное RTP-проксирование трафика;
- аутентификация VoIP-оборудования;
- поддержка VoIP-оборудования, работающего на NAT;
- удаленное управление через WEB-интерфейс;
- поддержка SNMP-интерфейса для сбора статистики и формирования сообщений об авариях;
- масштабируемая архитектура;
- автоматический рестарт при сбоях;
- поддержка резервирования.

Виртуальная функция: ИнфоТеКС ViPNet Coordinator VA

Программно-аппаратный комплекс ViPNet Coordinator HW (далее — ViPNet Coordinator HW) представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet, которое функционирует под управлением адаптированной ОС Linux.

ViPNet Coordinator HW реализует функции межсетевого экрана, VPN-шлюза, сервера IP-адресов и VPN-сервера в IP-сетях, защита которых организуется совместно с комплексом программных продуктов ViPNet. Предназначен для разграничения доступа

к сетевым узлам, защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.

ViPNet Coordinator HW также может выполнять дополнительные функции:

- Выступать в роли DHCP-, DNS- и NTP-серверов
- Выступать в роли прокси-сервера
- Обеспечивать защиту соединений между удаленными сегментами сети по технологии L2OverIP
- Обеспечивать обработку прикладных протоколов FTP, DNS, H.323, SCCP, SIP для всех видов трафика (защищенного, открытого и туннелируемого)

В качестве аппаратной платформы в ViPNet Coordinator HW может использоваться компактный компьютер или полноценный сервер, устанавливаемый в стандартные стойки. Существует также модификация, не зависящая от аппаратной платформы, — ViPNet Coordinator HW-VA. Это программное виртуализированное решение, предназначенное для разворачивания на виртуальной машине. ViPNet Coordinator HW-VA можно установить на одну из следующих платформ виртуализации: VMware Workstation, VMware vSphere или Oracle VM VirtualBox.

VPN-сервер в защищенной сети ViPNet называется координатором. Как правило, узел ViPNet Coordinator HW выполняет в сети одну или несколько функций в зависимости от задач, решаемых в рамках корпоративной сети, ее структуры, нагрузки на координатор и других факторов.

Координатор выполняет в защищенной сети ViPNet следующие функции:

- Сервер IP-адресов. Функция, которая позволяет обеспечить взаимодействие защищенных узлов ViPNet. Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.
- Маршрутизатор VPN-пакетов. Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы. В случае фильтрации и трансляции трафика сторонними устройствами координатор может выступать в роли сервера соединений.
- VPN-шлюз. Функция, которая позволяет создавать защищенные каналы (туннели) для организации защищенных соединений с открытыми узлами.
- Сервер-маршрутизатор. Функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами.
- Межсетевой экран. Функция, которая позволяет обеспечить фильтрацию открытого трафика. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.
- Сервер открытого Интернета. Функция, которая позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации.

3. Схема тестирования

Цель тестирования: осуществить настройку виртуальных функции отечественного производства и убедиться в корректности отработки базового функционала.

Составляющие элементы тестирования:

Наименование	Версия ПО	Кол-во
RAD ETX-2i/ACHP/19V	5.9.1(0.25)	2
RADview	5.0.1 (355)	1
ПРОТЕЙ mCore.MKD vPBX	4.2.7.13	1
ИнфоТеКС ViPNet Coordinator VA	4.1.2-1118	2

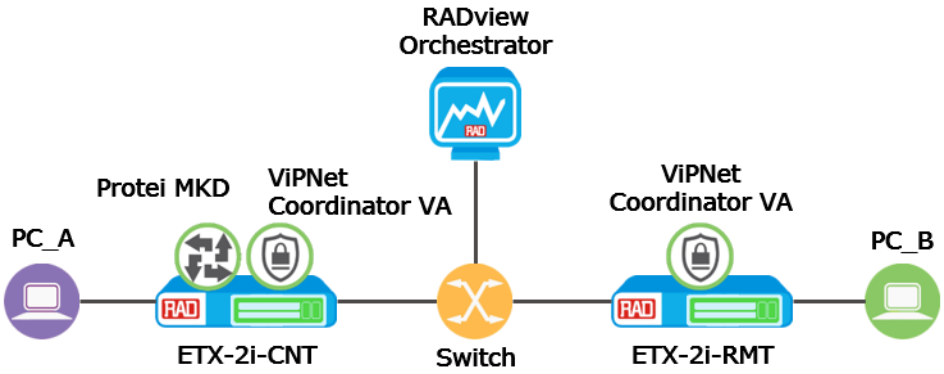
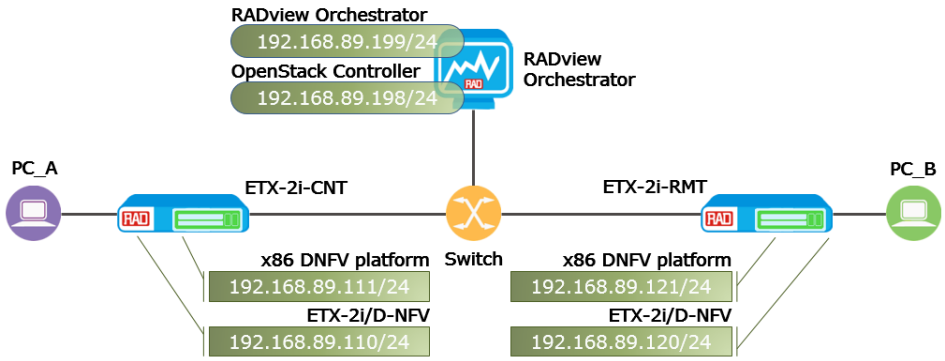


Рисунок 3: Схема тестирования концепции

4. Описание тестирования

Этап № 1: Подготовка сетевой инфраструктуры

Цели	Собрать тестовый стенд в лаборатории и настроить сетевую инфраструктуру для управления с помощью системы RADview
Критерии успеха	• Устройства RAD ETX могут пропинговать друг друга • Система управления RADview отображает все устройства RAD
Схема теста	Схема теста: 

Описание настроек

В данном этапе тестирования будут использоваться следующие IP адреса:

Устройство	IP адрес	Маска
ETX-2i-CNT	192.168.89.110	24
ETX-2i-CNT/x86	192.168.89.111	24
ETX-2i-RMT	192.168.89.120	24
ETX-2i-RMT/x86	192.168.89.121	24
RADview Orchestartor	192.168.89.199	24
OpenStack Controller	192.168.89.198	24

Для функционирования системы оркестрации необходима установка виртуальной машины (или отдельного сервера) для платформы OpenStack, которая осуществляет функции взаимодействия с платформами виртуализации. Сама оболочка RADview при этом осуществляет упрощенную графическую интерпретацию, необходимую для настройки и конфигурацию/провиженинг сетевой части решения.

Для настройки управления необходимо создать потоки для трафика менеджмента и прописать IP адреса.

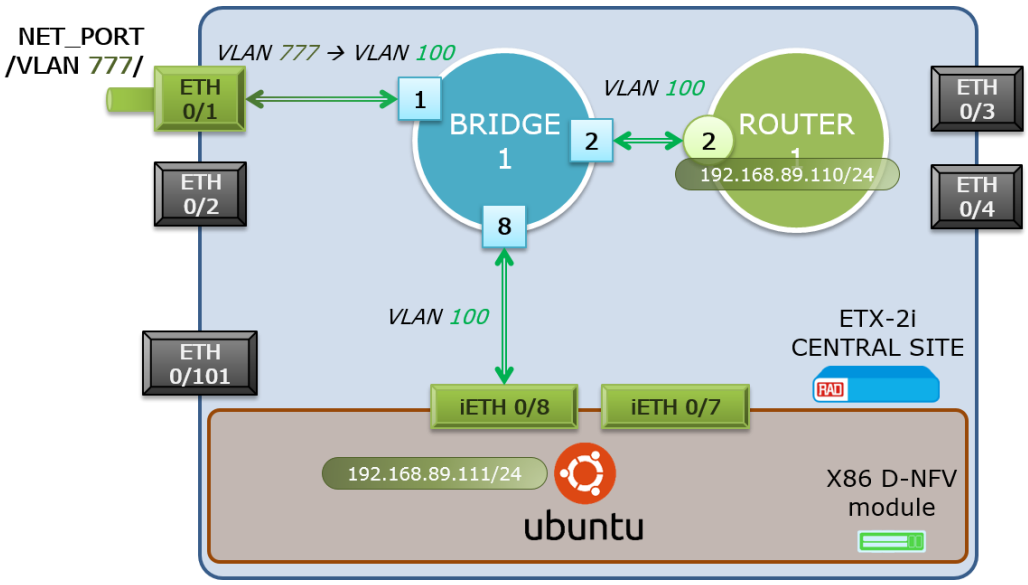


Рисунок 4: Схема организации потоков для управления

Управление устройства RAD ETX-2i настраивается с помощью следующих команд:

- Настройка имени устройства

```
configure system name ETX-2i-CNT
```

- Настройка тайм-аута терминальной сессии

```
configure terminal timeout forever
```

- Настройка физических портов

```
configure port
ethernet 0/1
name NET_PORT
no shutdown
exit all

configure port
ethernet 0/2
shutdown
exit all

configure port
ethernet 0/3
name USER_PORT
no shutdown
exit all

configure port
ethernet 0/4
shutdown
exit all
```

```
configure port
int-ethernet 0/7
name "X86_USER_PORT
no shutdown
exit all

configure port
ethernet 0/8
name "X86_NET_PORT"
no shutdown
exit all

configure port
ethernet 0/101
shutdown
exit all
```

- Настройка виртуального порта управления

```
configure port
svi 2
name MANAGEMENT
no shutdown
exit all
```

- Настройка портов внутреннего бриджа

```
configure bridge 1
port 1
no shutdown
exit all

configure bridge 1
port 2
no shutdown
exit all

configure bridge 1
port 8
no shutdown
exit all

configure bridge 1
vlan 777
exit all
```

- Настройка классификаторов трафика

```
configure flows classifier-profile class_all match-any
match all
exit all

configure flows classifier-profile class_mng match-any
match vlan 777
exit all

configure flows classifier-profile class_x86_mng match-any
match vlan 100
exit all

configure flows classifier-profile class_untagged match-any
match untagged
exit all
```

- Настройка потоков передачи данных

```
configure flows
flow mng_eth1_bp1
classifier class_mng
mark all
vlan 100
exit
ingress-port ethernet 0/1
egress-port bridge-port 1 1
reverse-direction block 0/1
no shutdown
exit all

configure flows
flow mng_svi2_bp2
classifier class_all
ingress-port svi 2
egress-port bridge-port 1 2
vlan-tag push vlan 100 p-bit fixed 7
reverse-direction
no shutdown
exit all

configure flows
flow mng_ieth8_bp8
classifier class_x86_mng
ingress-port int-ethernet 0/8
```

```
egress-port bridge-port 1 8
reverse-direction block 0/1
no shutdown
exit all
```

- Настройка интерфейса внутреннего маршрутизатора

```
configure router 1 interface 1
no dhcp
bind svi 2
address 192.168.89.110/24
no shutdown
exit
static-route 0.0.0.0/0 address 192.168.89.1
exit all
```

- Настройка параметров SNMPv3

```
configure management snmp
view internet 1
mask 1
type included
no shutdown
exit all

configure management snmp
access-group initial usm no-auth-no-priv
context-match prefix
exit all

configure management snmp
target-params SNMP_V3
message-processing-model snmpv3
version usm
security name initial level no-auth-no-priv
no shutdown
exit all

configure management snmp
target NMS_snmpv3
target-params SNMP_V3
tag-list unmasked
address udp-domain 192.168.89.199
no shutdown
exit all
```

```
configure management snmp
notify unmasked
tag unmasked
no shutdown
exit all
```

- Настройка параметров NTP

```
configure system date-and-time
zone utc +03:00
sntp
server 1
address 194.190.168.1
prefer
no shutdown
query-server
exit all
```

Аналогичные настройки осуществляются на устройстве ETX-2i-RMT.

После настройки ETX-2i нужно присвоить адрес управления x86 модулю с помощью следующих команд:

- Перейти к настройкам x86 модуля из-под CLI ETX'a

```
configure chassis ve-module remote-terminal
```

- Получив доступ к x86 модулю, необходимо ввести базовую конфигурацию с помощью скрипта

```
dnfv-conf --ip=192.168.89.111 --mask=255.255.255.0 --ip-
ctrl=192.168.89.198
```

- Перезагрузить x86 модуль

На промежуточном коммутаторе необходимо настроить VLAN'ы: 777 (управление устройствами), 778 (управление виртуальными функциями) и 100 (передача клиентских данных).

В системе RADview необходимо добавить устройства на карту.

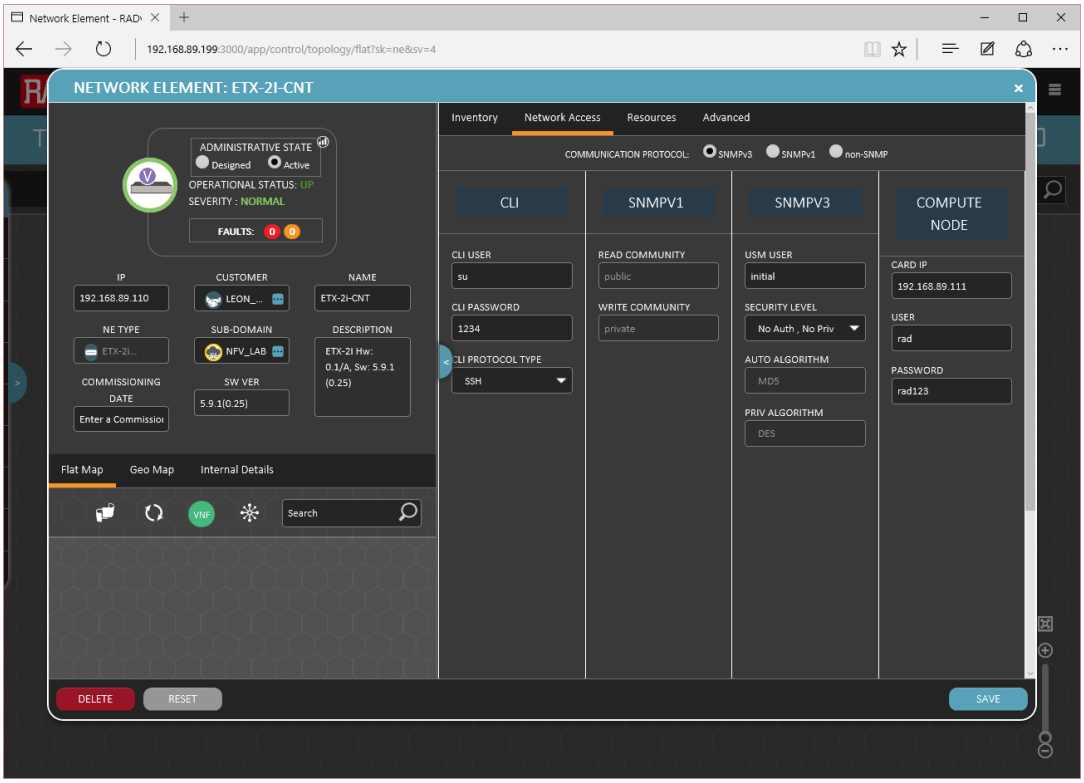


Рисунок 5: Окно настройки сетевого устройства

Результат

- Устройства пингуют друг друга
- Устройства отображаются на карте сети в системе RADview

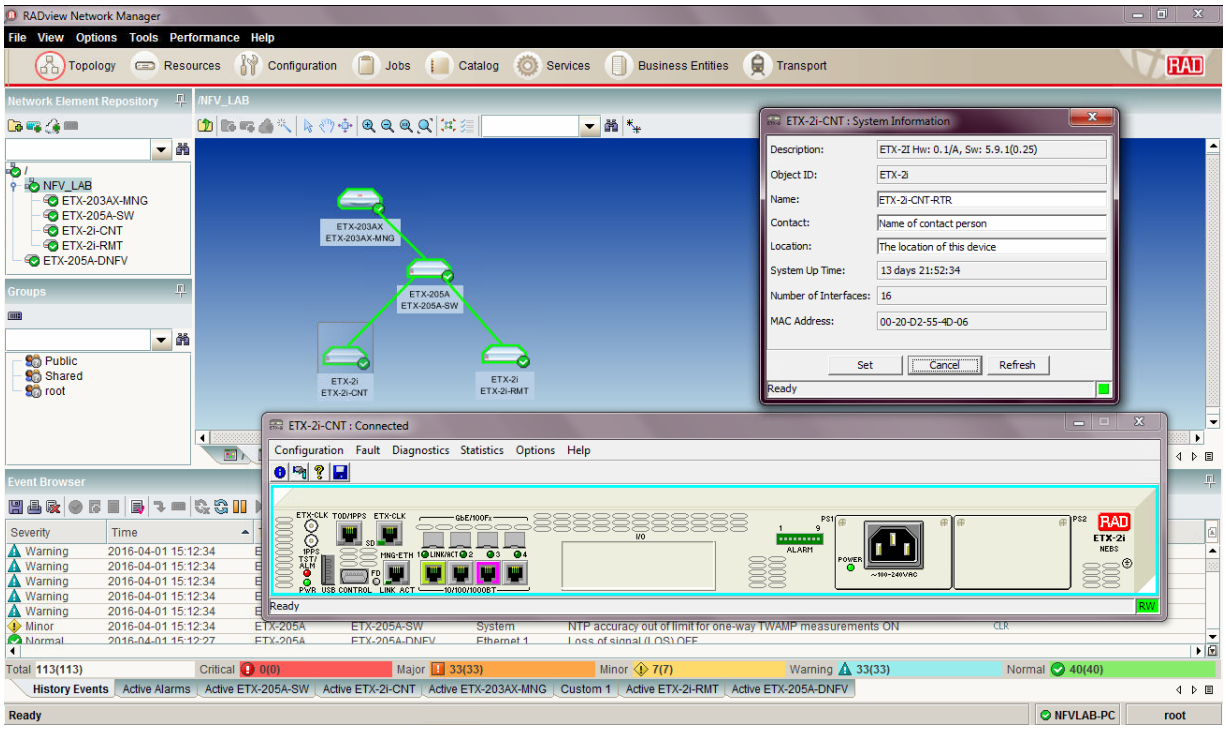


Рисунок 6: Отображение устройств в «классическом» клиенте RADview

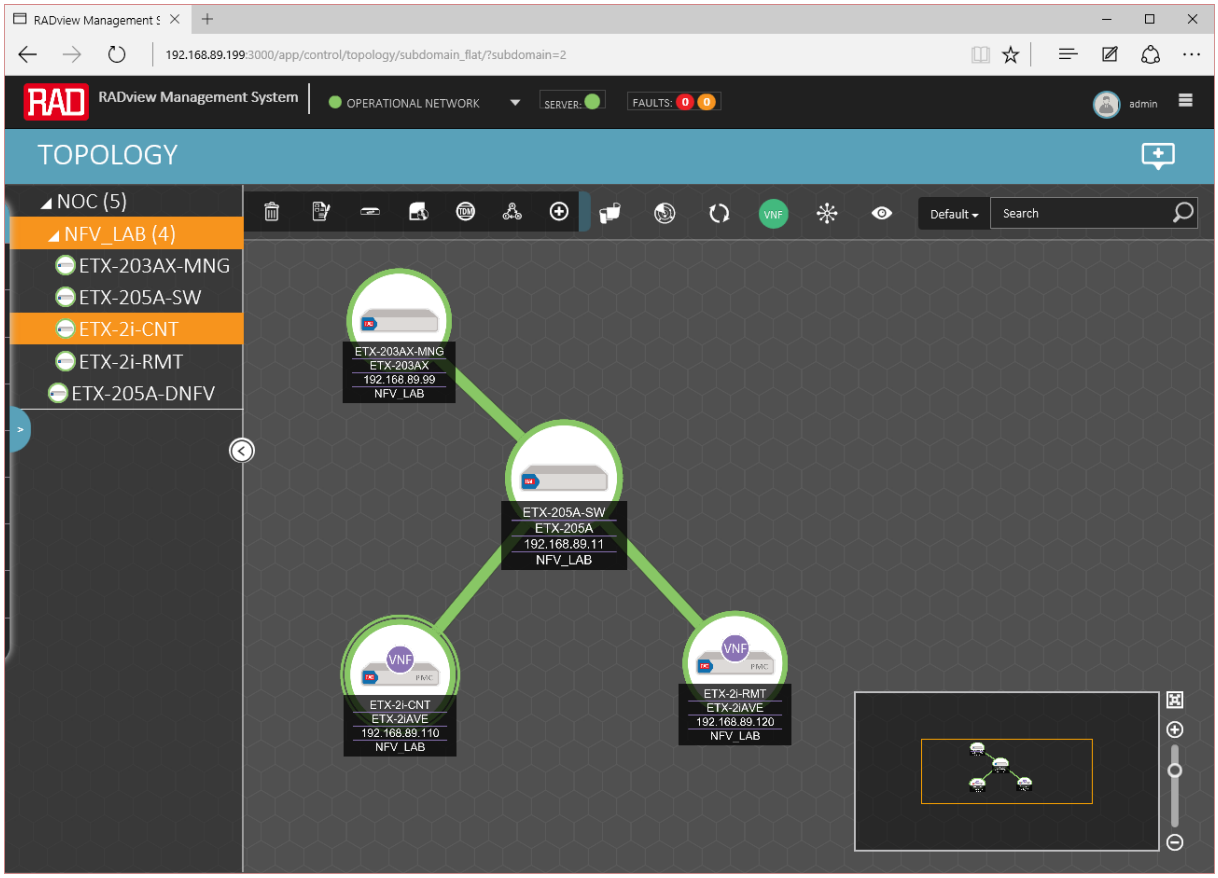


Рисунок 7: Отображение устройств в обновленном web-интерфейсе RADview

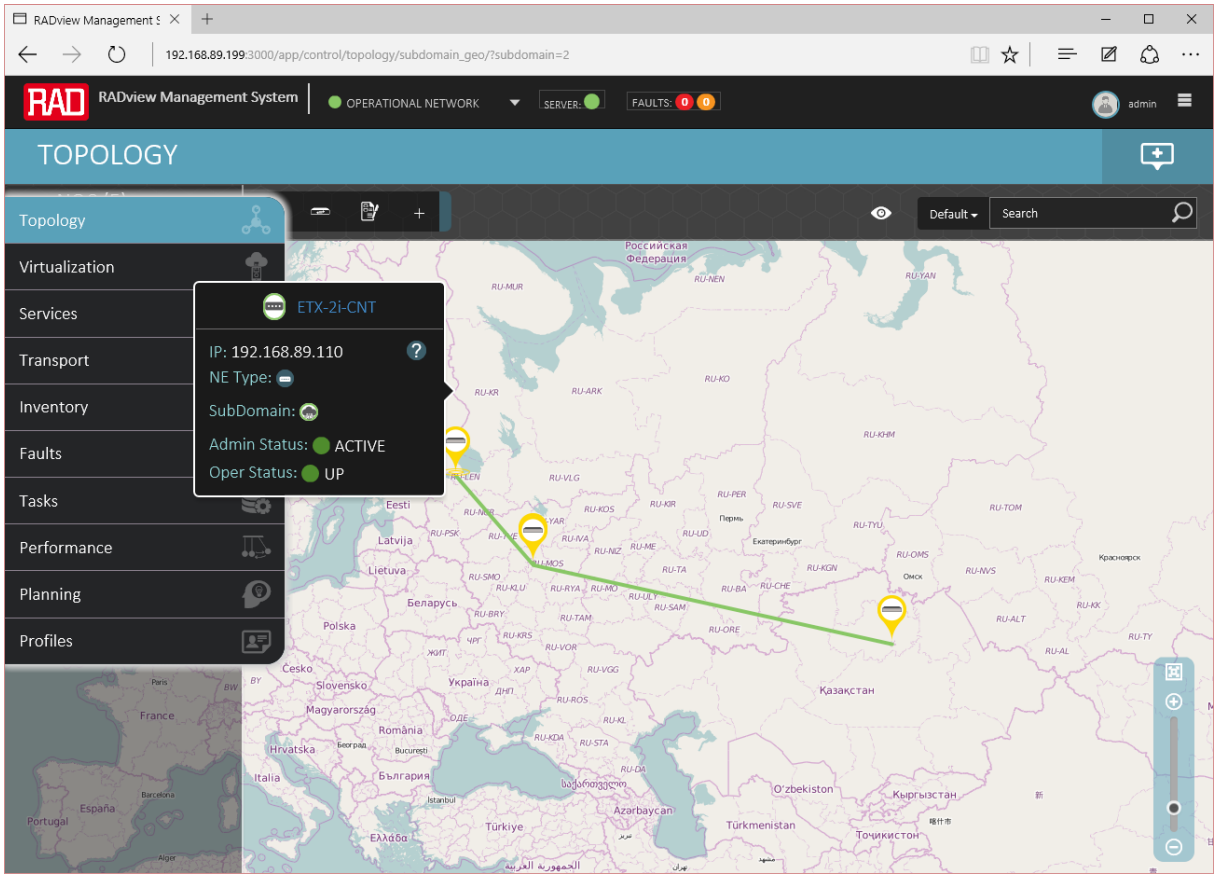
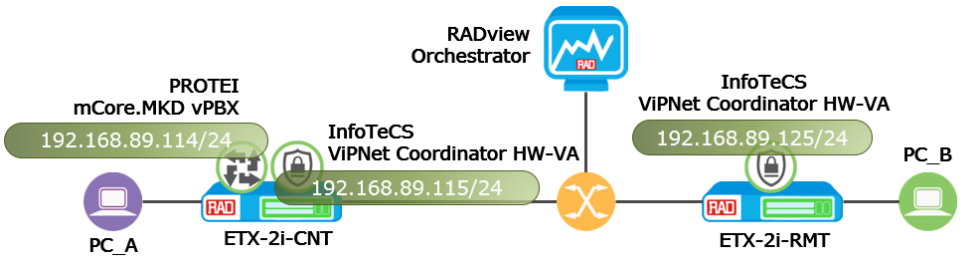


Рисунок 8: Отображение устройств на карте

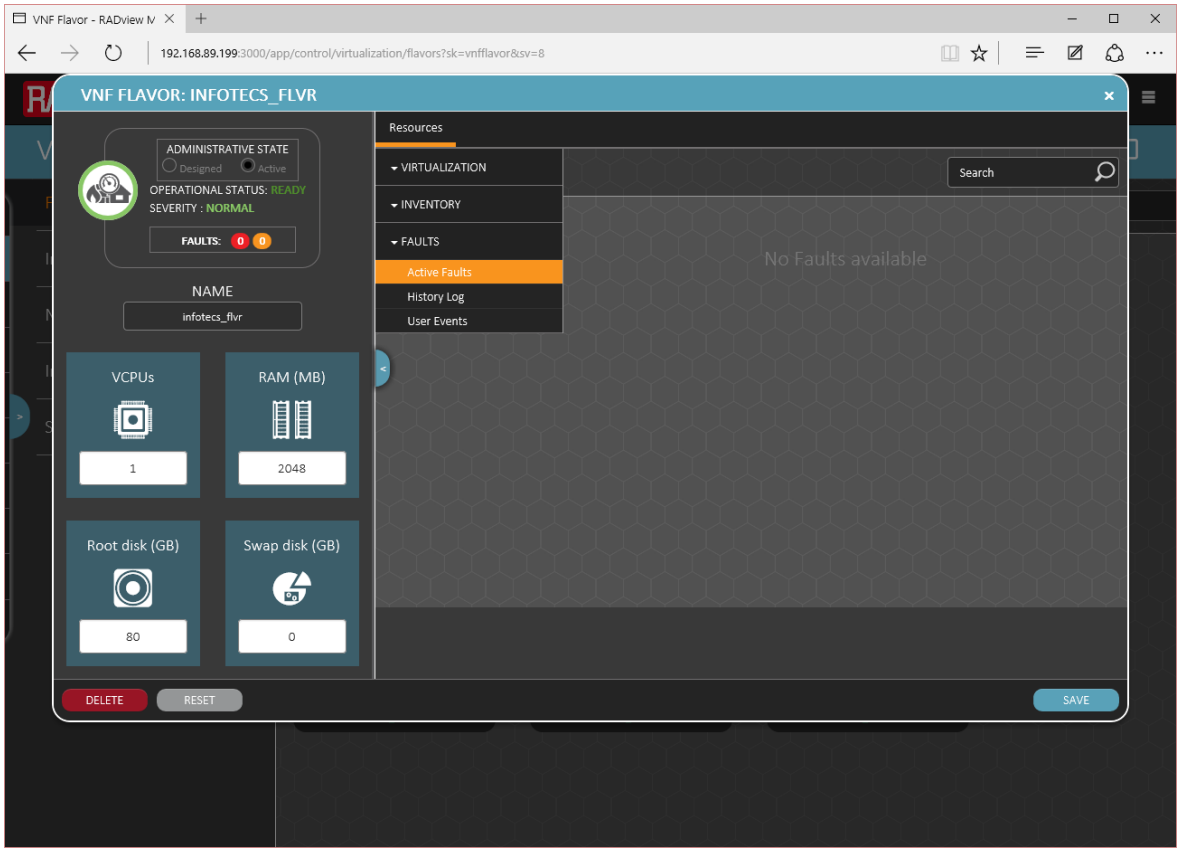
Этап № 2: Создание виртуальных функций

Цели	Запустить виртуальные функции на x86 модуле для обоих устройств ETX
Критерии успеха	• На обоих ETX'ах успешно развернуты виртуальные функции • Командный интерфейс виртуальных функций доступен через встроенную консоль
Схема теста	Схема теста: 

Описание настроек

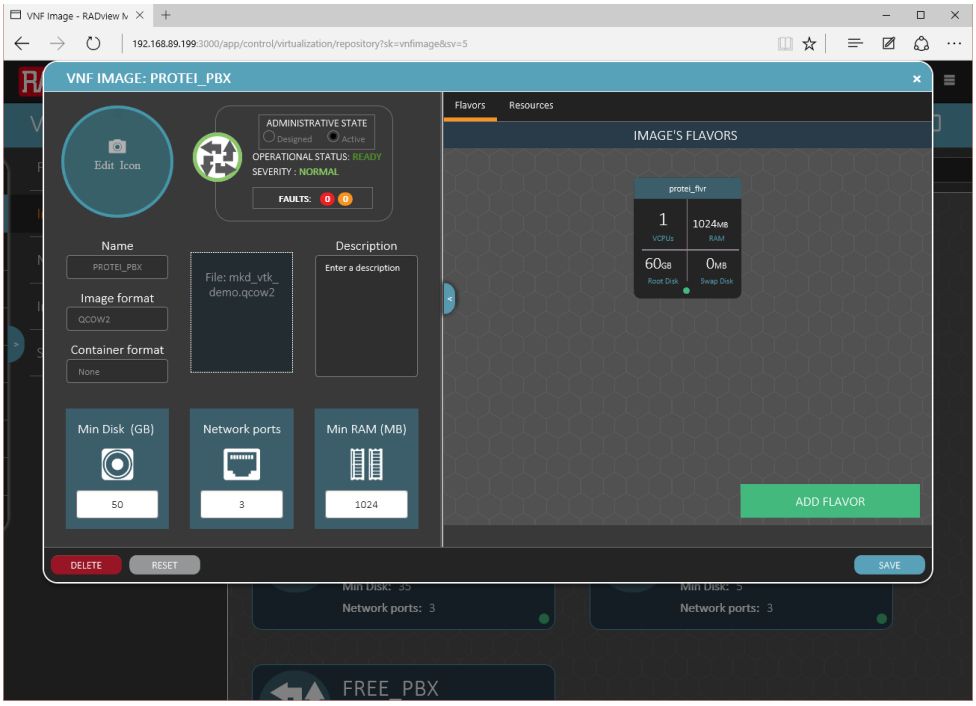
Для создания виртуальных функций воспользуемся web-интерфейсом системы оркестрации RADview:

- Создать шаблон параметров виртуальной машины

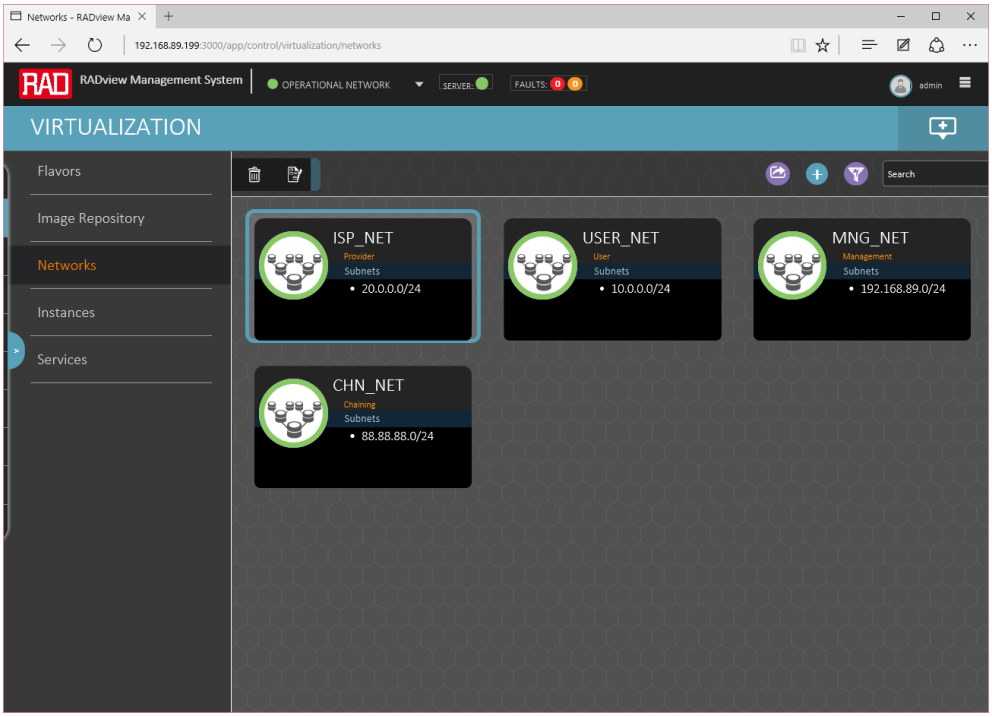


Функция	VCPUs	RAM (MB)	Root disk (GB)	Swap disk (GB)
ИнфоТеКС ViPNet Coordinator VA	1	2048	80	0
ПРОТЕЙ mCore.MKD VPBX	1	1024	60	0

- Загрузить образы в систему оркестрации RADview (для функции ViPNet Coordinator VA были использованы отдельные преднастроенные образы для каждого узла)

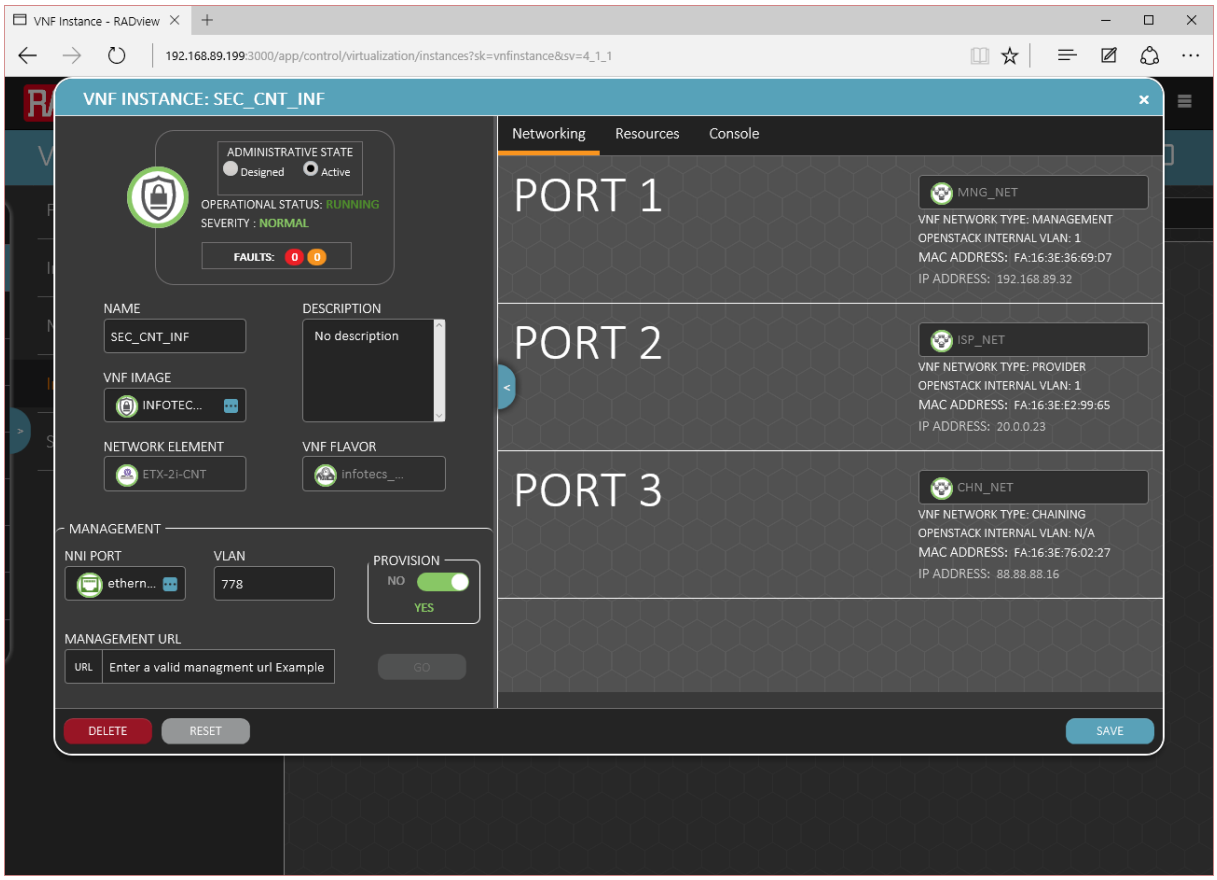


- Создать логические профили сетей для распределения ролей виртуальных портов внутри платформы виртуализации



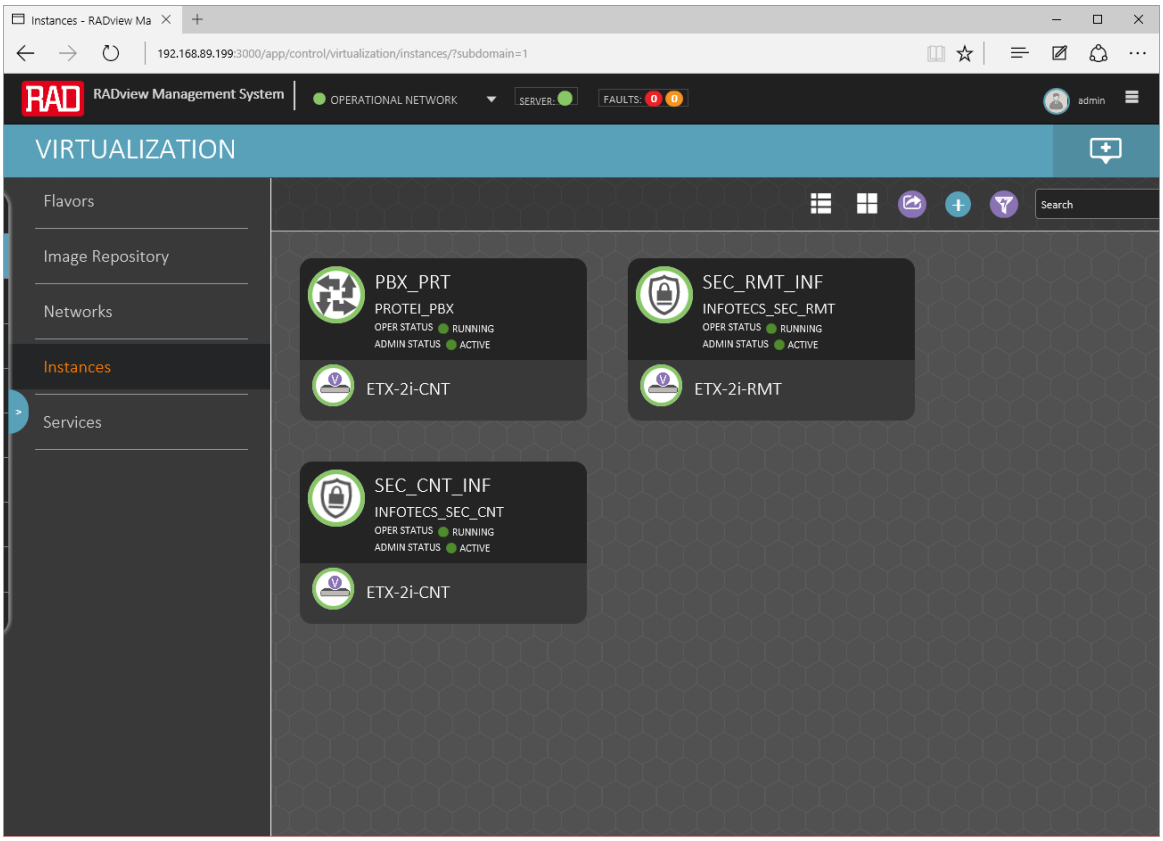
- Создать виртуальную машину на основе ранее введенных шаблонов. В настройке сетевых параметров необходимо указать роль портов виртуальной машины на основе ранее созданных шаблонов сетей. См. ниже таблицу виртуальных функций.

Виртуальная машина	Образ	Порт	Роль	Назначение
SEC_CNT_INF	INFOTECS_SEC	1	MNG_NET	Порт управления
		2	ISP_NET	Сетевой порт функции
		3	CHN_NET	Порт для связывания виртуальных функций (пользовательский порт)
PBX_PRT	PROTEI_PBX	1	MNG_NET	Порт управления
		2	CHN_NET	Порт для связывания виртуальных функций (сетевой порт)
		3	USER_NET	Пользовательский порт функции
SEC_RMT_INF	INFOTECS_SEC	1	MNG_NET	Порт управления
		2	ISP_NET	Сетевой порт функции
		3	USER_NET	Пользовательский порт функции

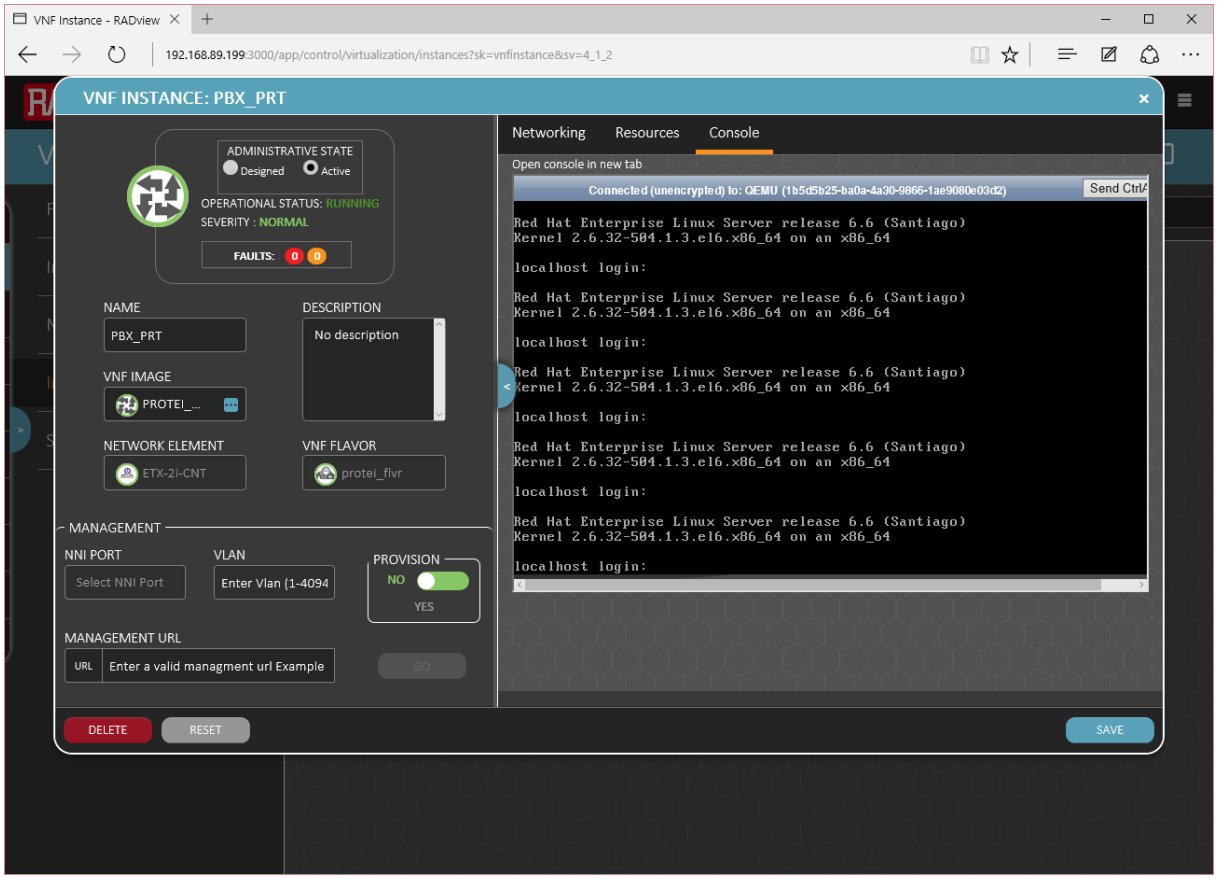


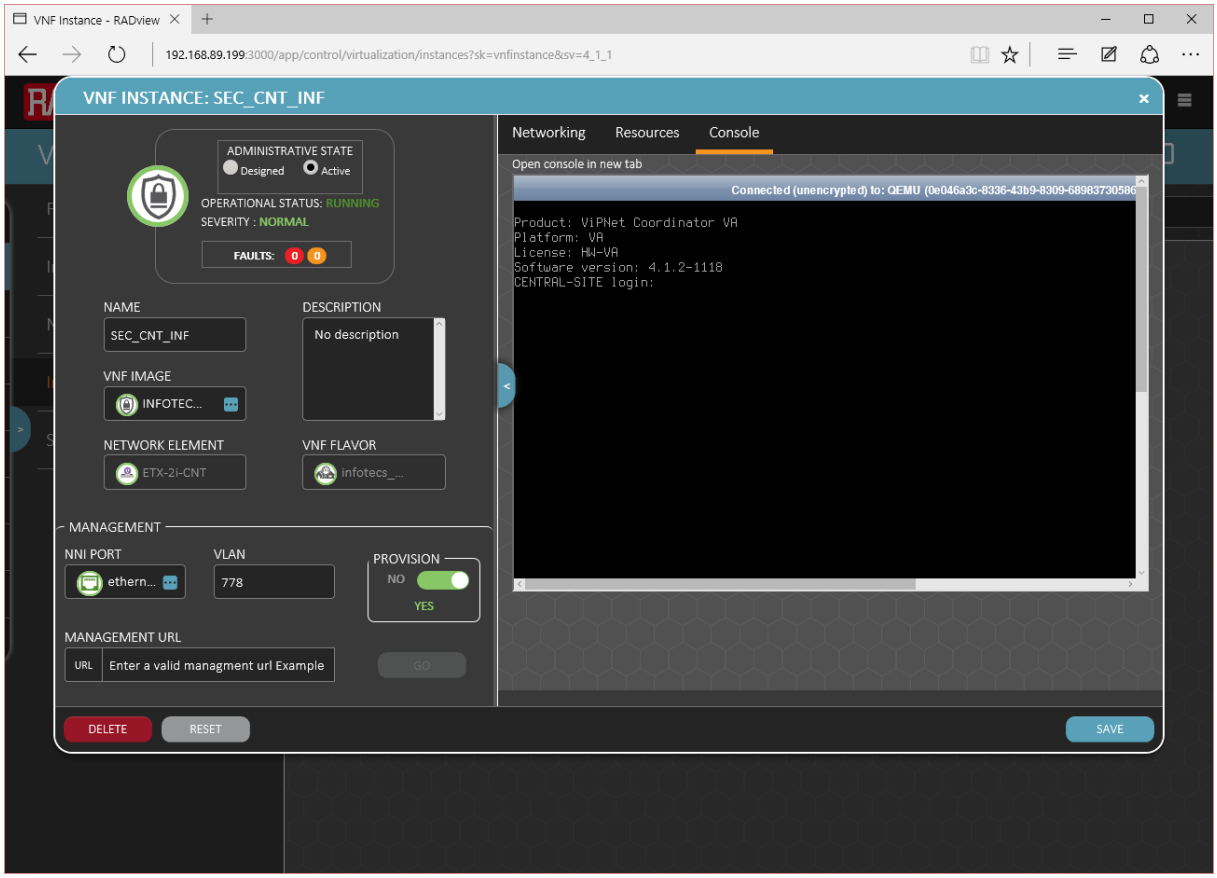
Результат

- В системе оркестрации все виртуальные машины активны и работают

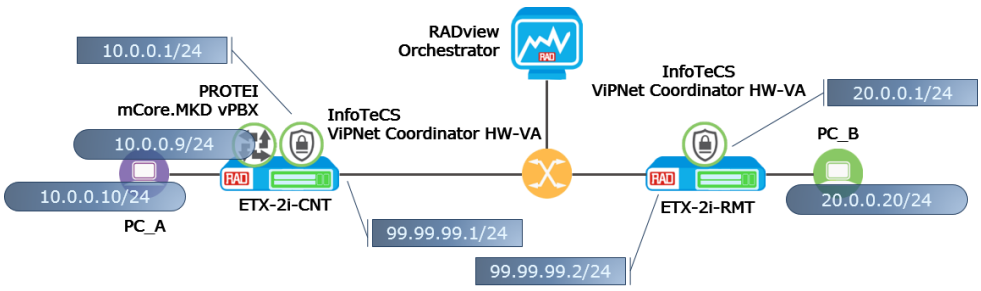


- Виртуальные машины доступны через консоль оркестратора





Этап № 3: Конфигурация виртуальных функций

Цели	Осуществить полную конфигурацию виртуальных функций для последующего создания сервисов
Критерии успеха	Виртуальные функции доступны по IP для управления
Схема теста	Схема теста: 

Описание настроек

Поскольку ПО ИнфоТеКС ViPNet Coordinator VA требует установки ключей локальным образом мы создали и преднастроили два образа виртуальной машины: для центрального узла и удаленного. ПО настроено таким образом, чтобы создавать шифрованный по ГОСТу VPN туннель между двумя ETX-2i.

Для настройки виртуальной IP АТС мы создадим несколько интерфейсов со следующими функциями:

Интерфейс	Назначение	Конфигурация
eth1	Управление	**DEVICE=eth1** **BOOTPROTO=none** **NETMASK=255.255.255.0** **TYPE=Ethernet** **HWADDR=fa:16:3e:98:82:1d** **IPADDR=192.168.89.114** **IPV6INIT=no** **ONBOOT=yes** **USERCTL=no**
eth2	Связка с другой виртуальной функцией	**DEVICE=eth2** **BOOTPROTO=none** **TYPE=Ethernet** **HWADDR=fa:16:3e:94:84:1f** **ONBOOT=yes** **IPV6INIT=no** **USERCTL=no** **BRIDGE=br0**
eth3	Пользовательский порт	**DEVICE=eth3** **BOOTPROTO=none** **TYPE=Ethernet** **HWADDR=fa:16:3e:1e:e1:bf** **ONBOOT=yes** **IPV6INIT=no** **USERCTL=no** **BRIDGE=br0**
br0	Мост, объединяющий интерфейсы eth2 и eth3	**DEVICE=br0** **BOOTPROTO=none** **TYPE=Bridge** **IPADDR=10.0.0.9** **NETMASK=255.255.255.0** **ONBOOT=yes**

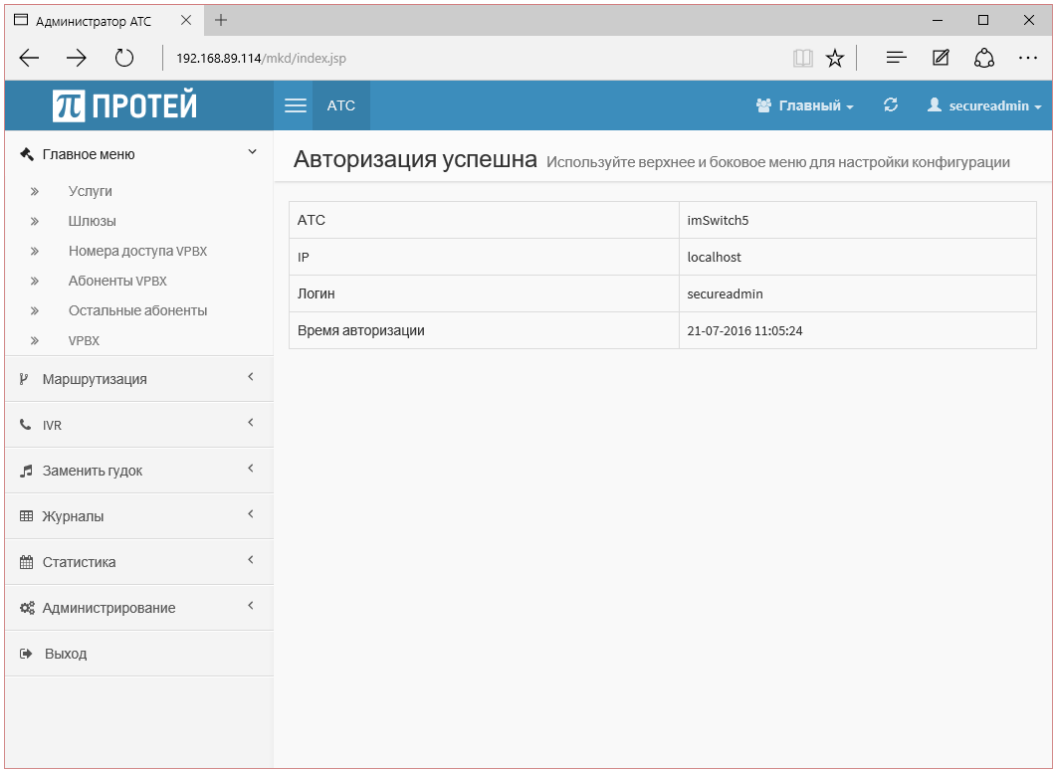
После изменения IP адреса необходимо запустить скрипт смены адреса в сетевых настройках IP-АТС и перезагрузить ПО

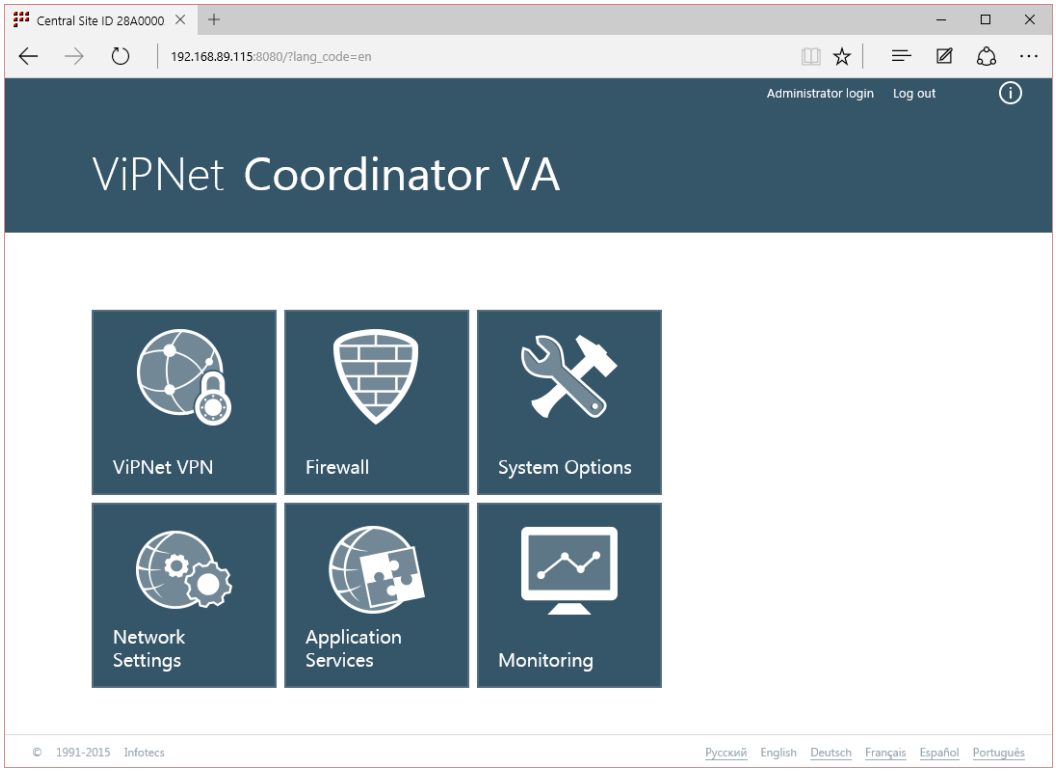
```
/usr/protei/Protei-MKD/change_MKD_IP.sh mkd {new_ip} {old_ip}
```

```
/usr/protei/Protei-MKD/change_MKD_IP.sh mcu {new_ip} {old_ip}
service protei-mkd restart service protei-mkd-mcu restart
```

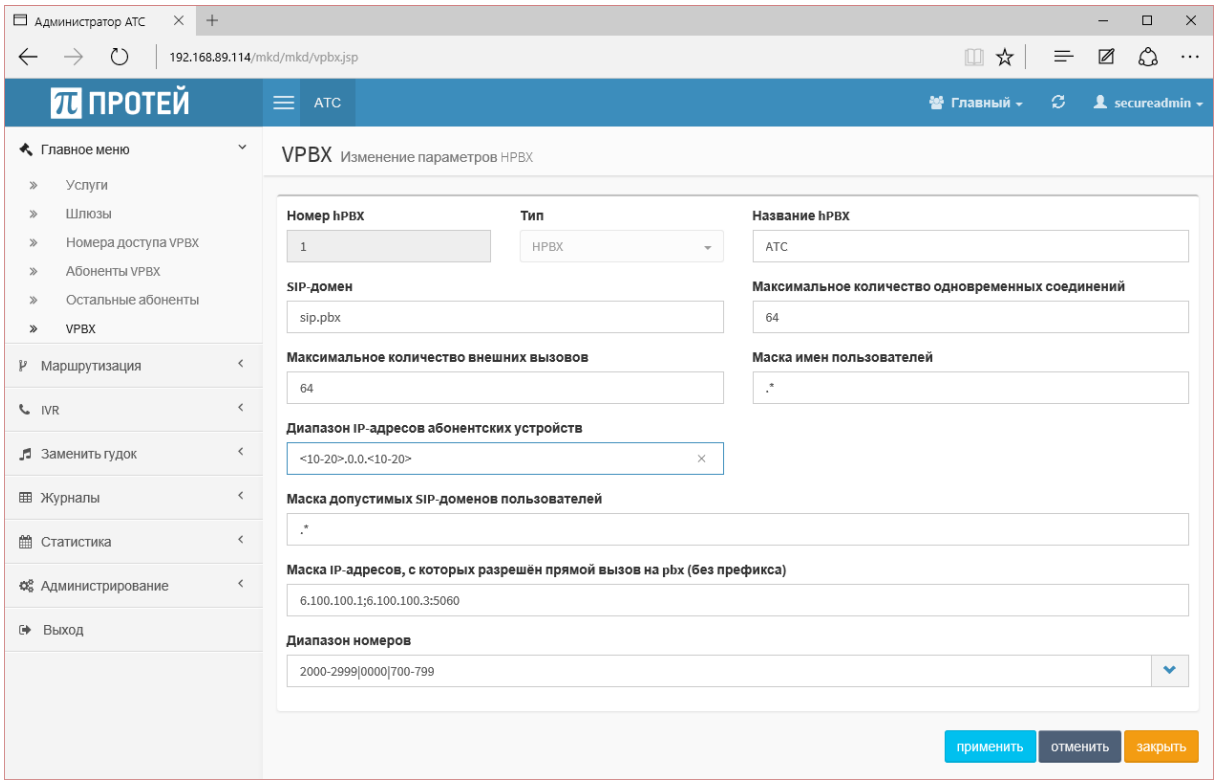
Результат

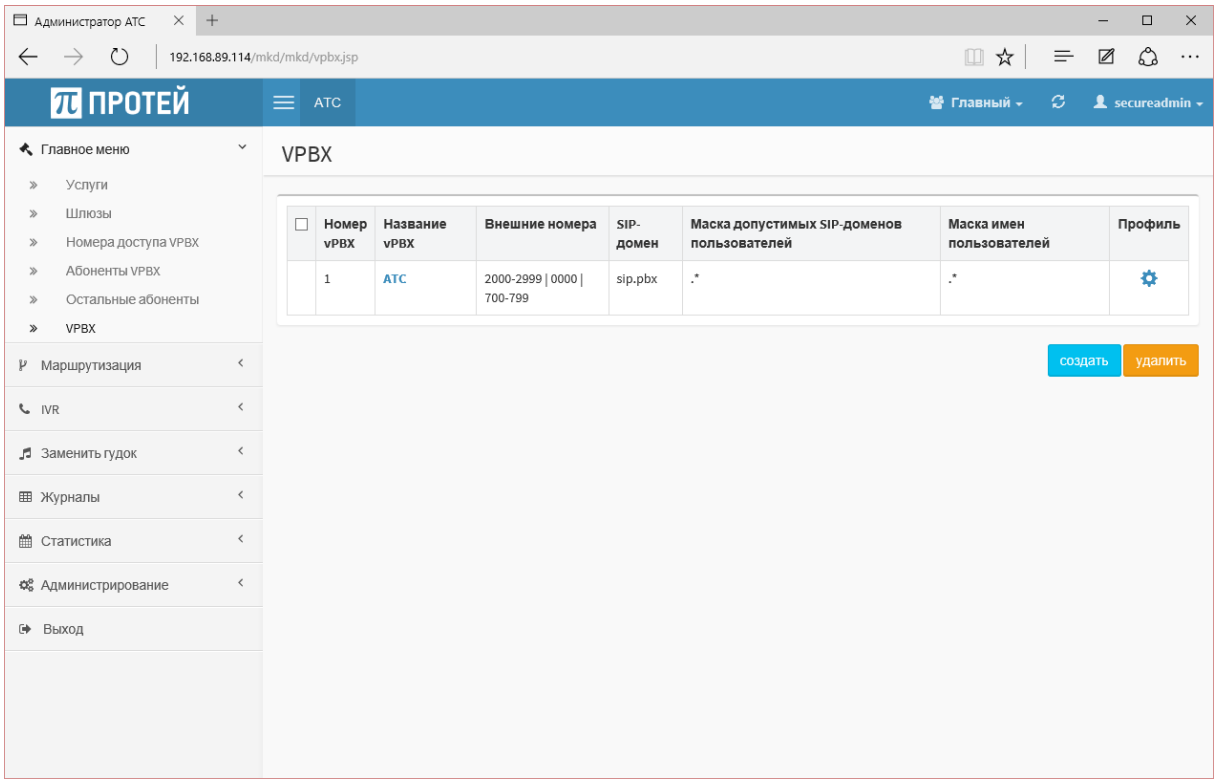
- Все три виртуальные функции доступны по IP для управления и имеют web-интерфейс



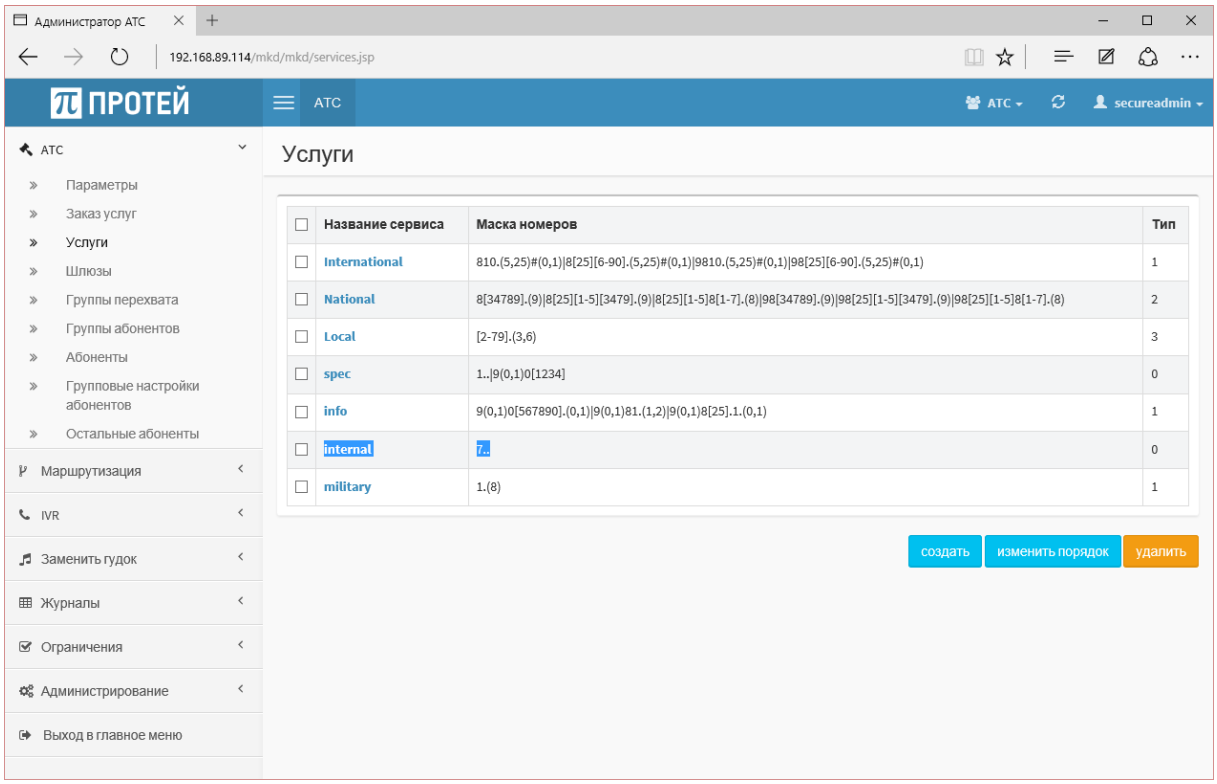


- Для начала осуществим настройки IP АТС в разделе vPBX, указав диапазоны IP-адресов абонентских устройств и диапазон номеров

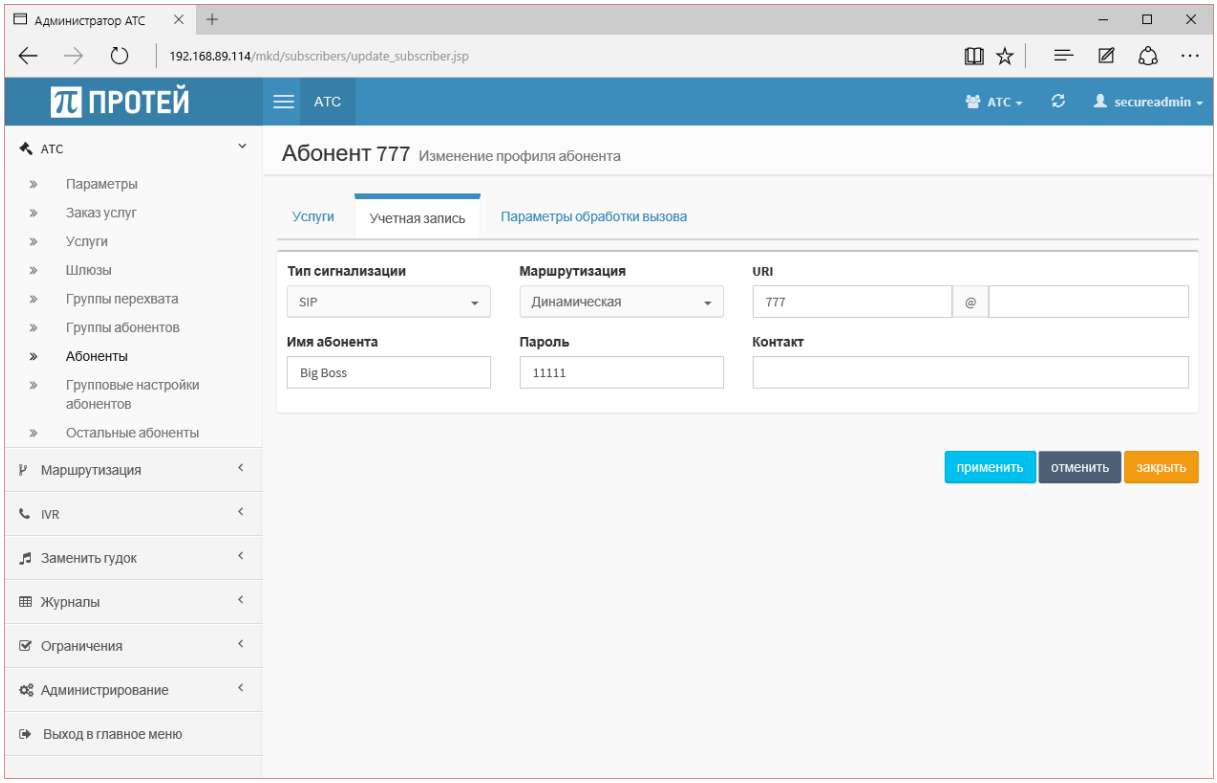


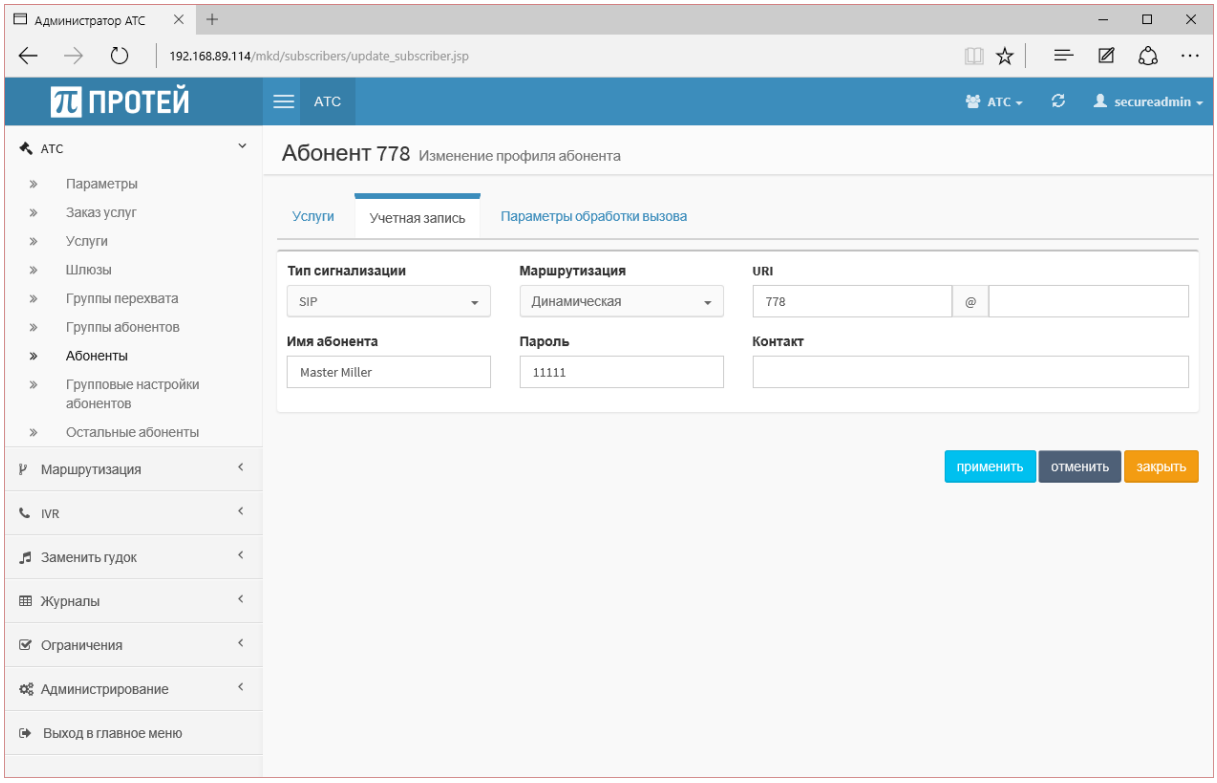


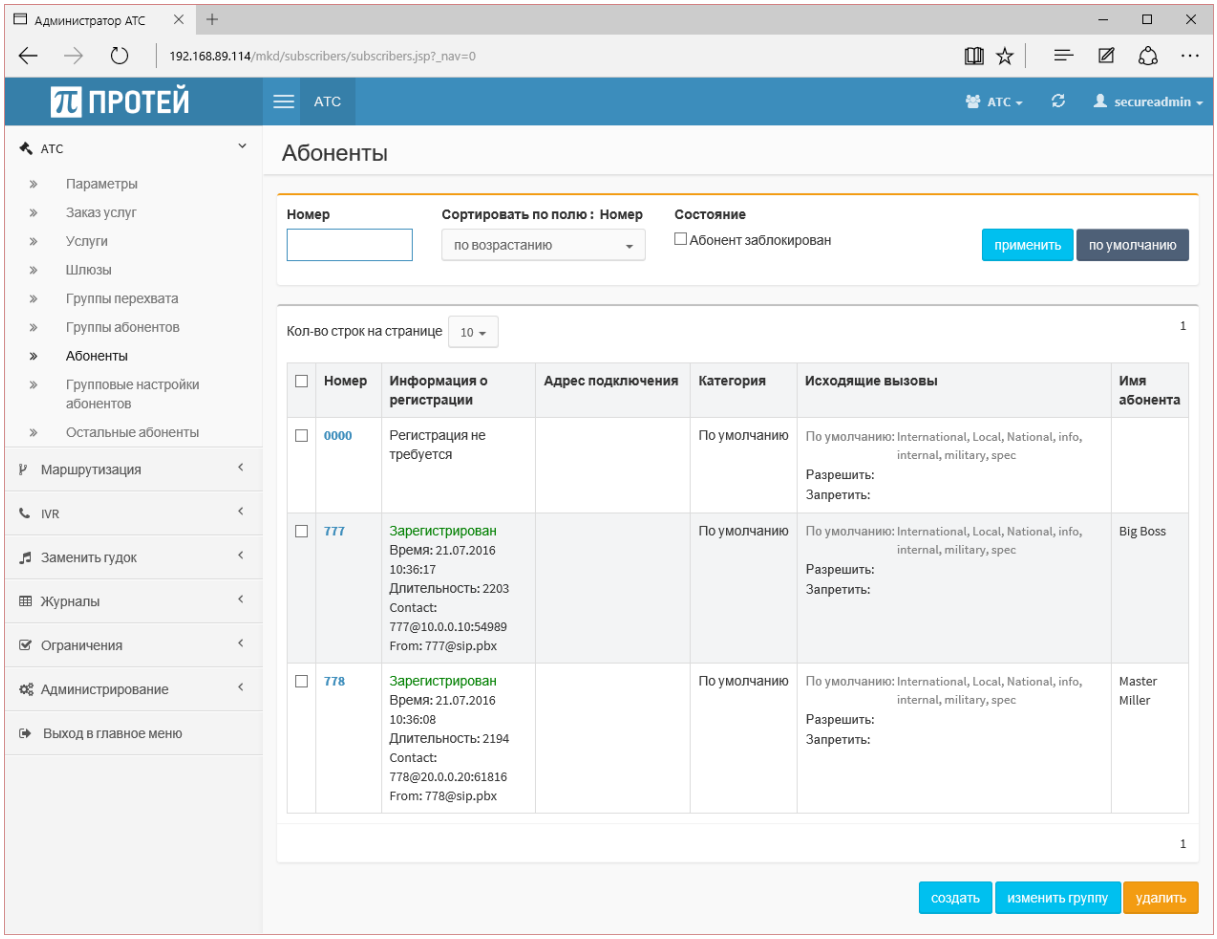
- Зайдя в настройки профиля vPBX, также настроим диапазон внутренних номеров телефонов



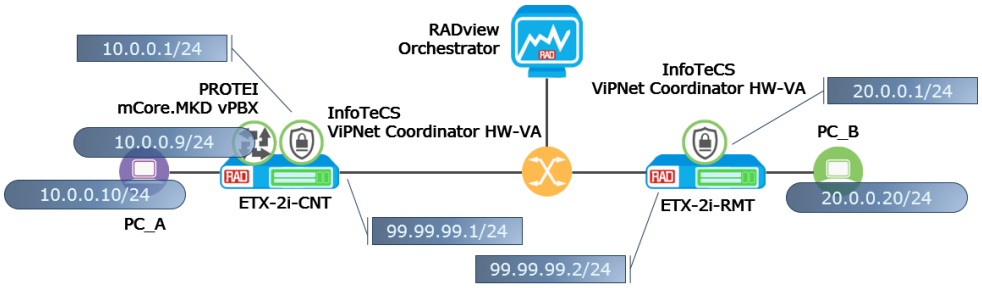
- Для IP АТС мы можем создать абонентов с номерами 777 и 778 (пароль для доступа к услуге - 11111)




Администратор АТС
192.168.89.114/mkd/subscribers/update_subscriber.jsp
ПРОТЕЙ
АТС
АТС
secureadmin
АТС
Параметры
Заказ услуг
Услуги
Шлюзы
Группы перехвата
Группы абонентов
Абоненты
Групповые настройки абонентов
Остальные абоненты
Маршрутизация
IVR
Заменить гудок
Журналы
Ограничения
Администрирование
Выход в главное меню
Абонент 778 Изменение профиля абонента
Услуги
Учетная запись
Параметры обработки вызова
Тип сигнализации
SIP
Маршрутизация
Динамическая
URI
778
@
Имя абонента
Master Miller
Пароль
11111
Контакт
применить
отменить
закрыть


Администратор АТС
192.168.89.114/mkd/subscribers/subscribers.jsp?_nav=0
ПРОТЕЙ
АТС
АТС
secureadmin
Абоненты
Номер
Сортировать по полю : Номер
по возрастанию
Состояние
Абонент заблокирован
применить
по умолчанию
Кол-во строк на странице 10
Номер
Информация о регистрации
Адрес подключения
Категория
Исходящие вызовы
Имя абонента
0000
Регистрация не требуется
По умолчанию
По умолчанию: International, Local, National, info, internal, military, spec
Разрешить:
Запретить:
777
Зарегистрирован
Время: 21.07.2016 10:36:17
Длительность: 2203
Contact: 777@10.0.0.10:54989
From: 777@sip.pbx
По умолчанию
По умолчанию: International, Local, National, info, internal, military, spec
Разрешить:
Запретить:
Big Boss
778
Зарегистрирован
Время: 21.07.2016 10:36:08
Длительность: 2194
Contact: 778@20.0.0.20:61816
From: 778@sip.pbx
По умолчанию
По умолчанию: International, Local, National, info, internal, military, spec
Разрешить:
Запретить:
Master Miller
создать
изменить группу
удалить

Этап № 4: Создание сервиса

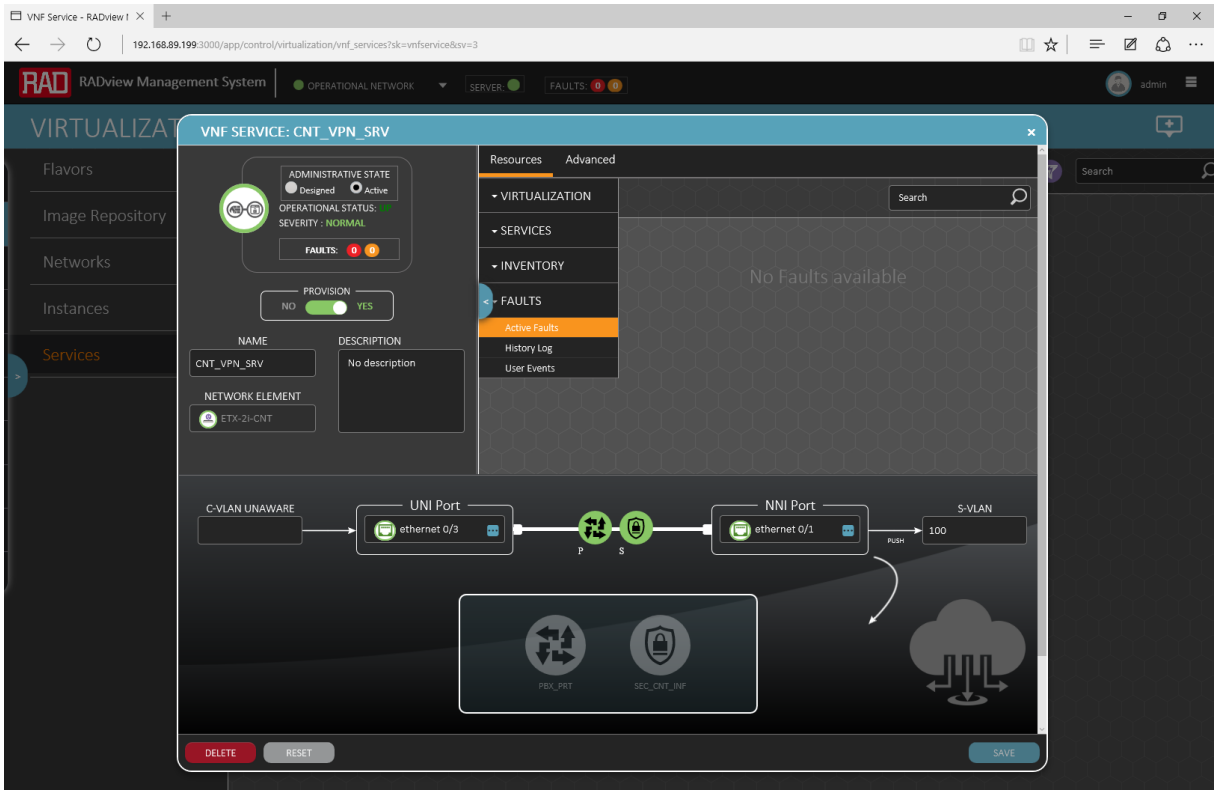
Цели	Обеспечить связность клиентских ПК между собой через канал, пролегающий через виртуальные функции
Критерии успеха	Абонентские ПК могут пинговать друг друга
Схема теста	Схема теста: 

Описание настроек

Для создания клиентских сервисов воспользуемся web-интерфейсом системы оркестрации RADview:

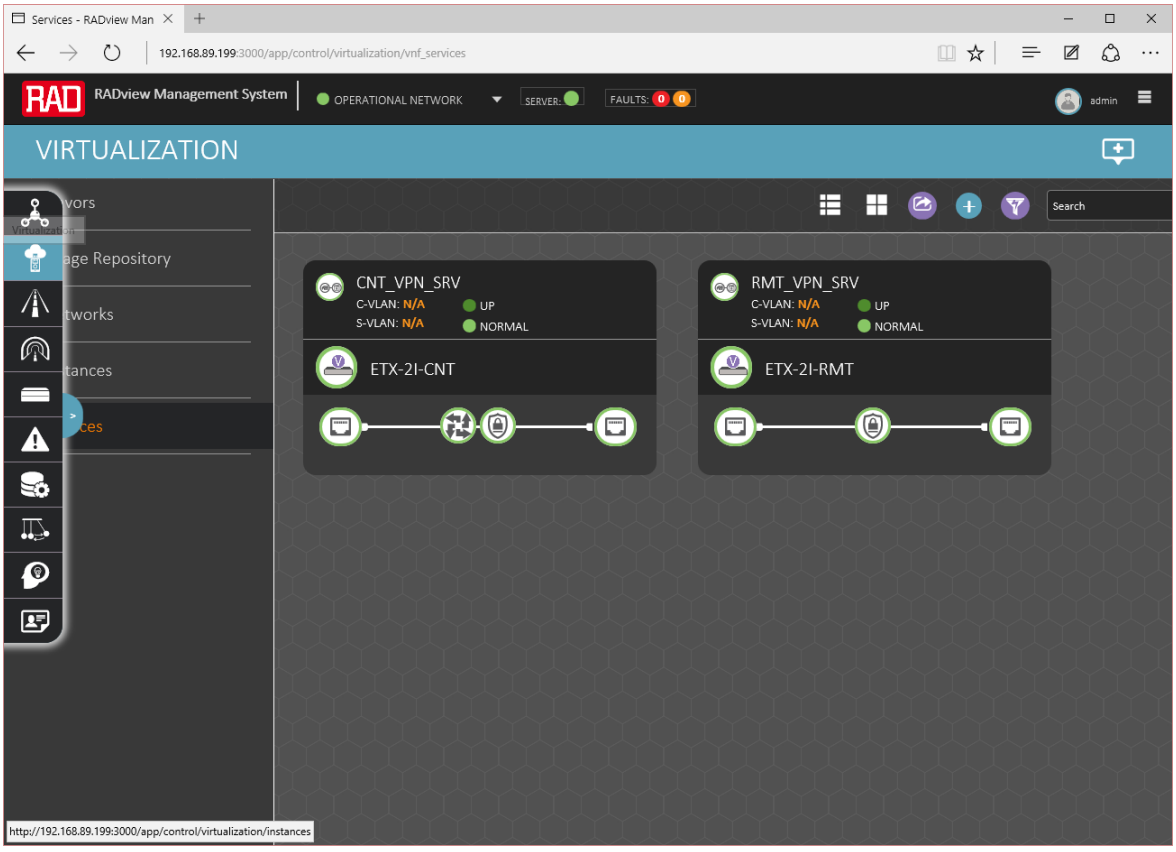
- Создадим сервис для удаленного узла

- Создадим сервис для центрального узла

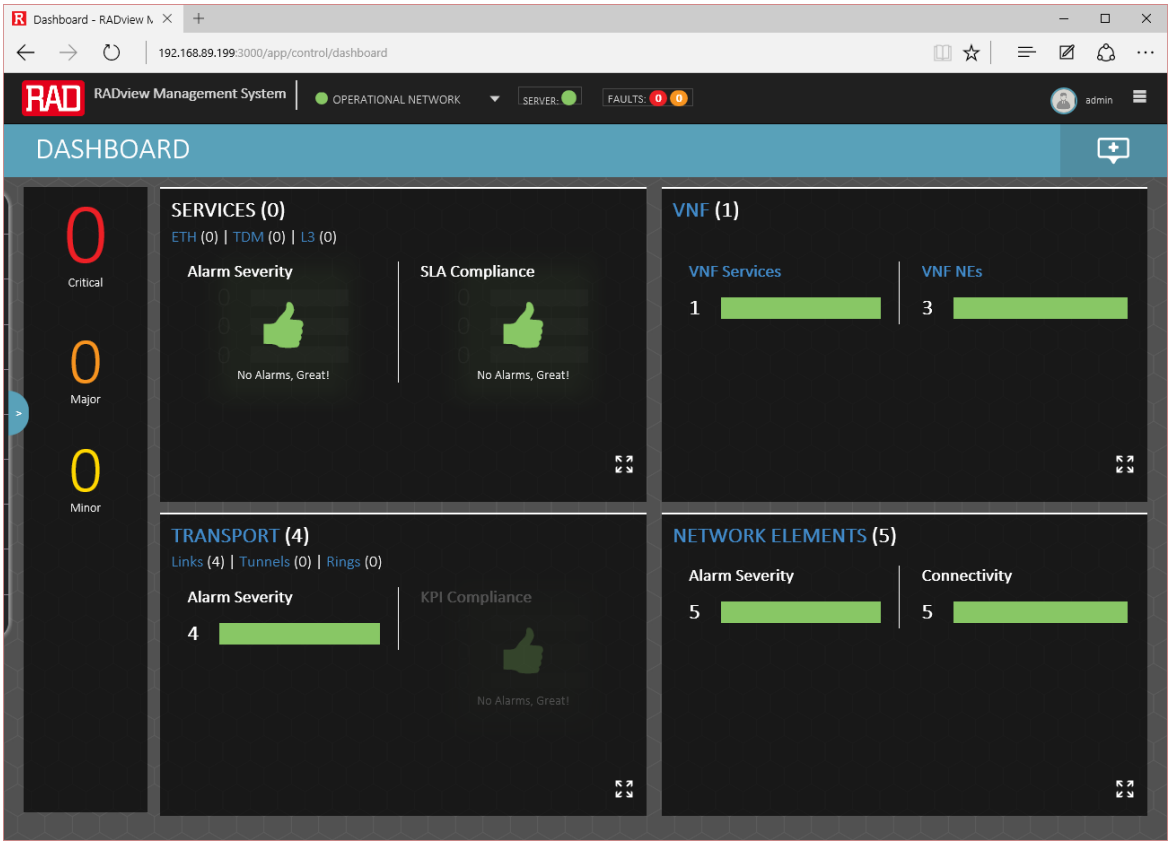


Результат

- Убедимся, что оба сервиса успешно созданы



- Убедимся, что в системе нет ошибок



- Убедимся, что оба клиентских ПК могут пинговать друг друга

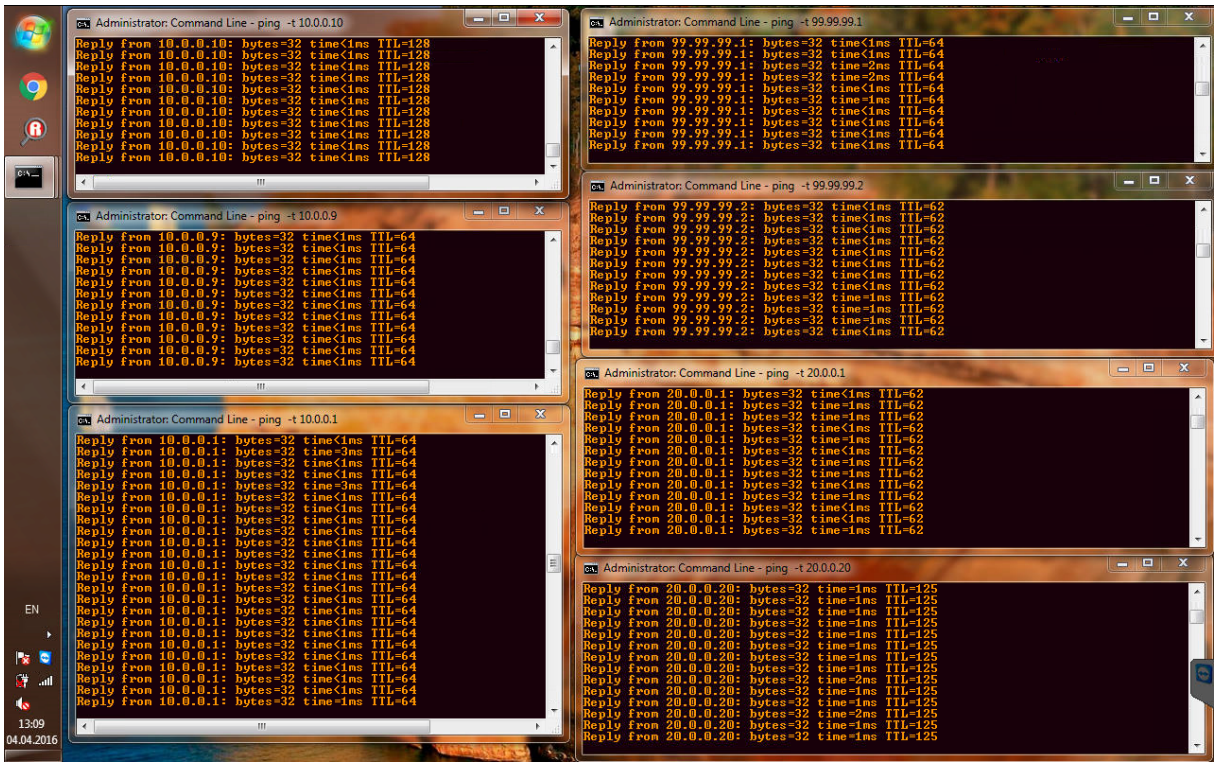


Рисунок 9: Пинги с компьютера PC_A

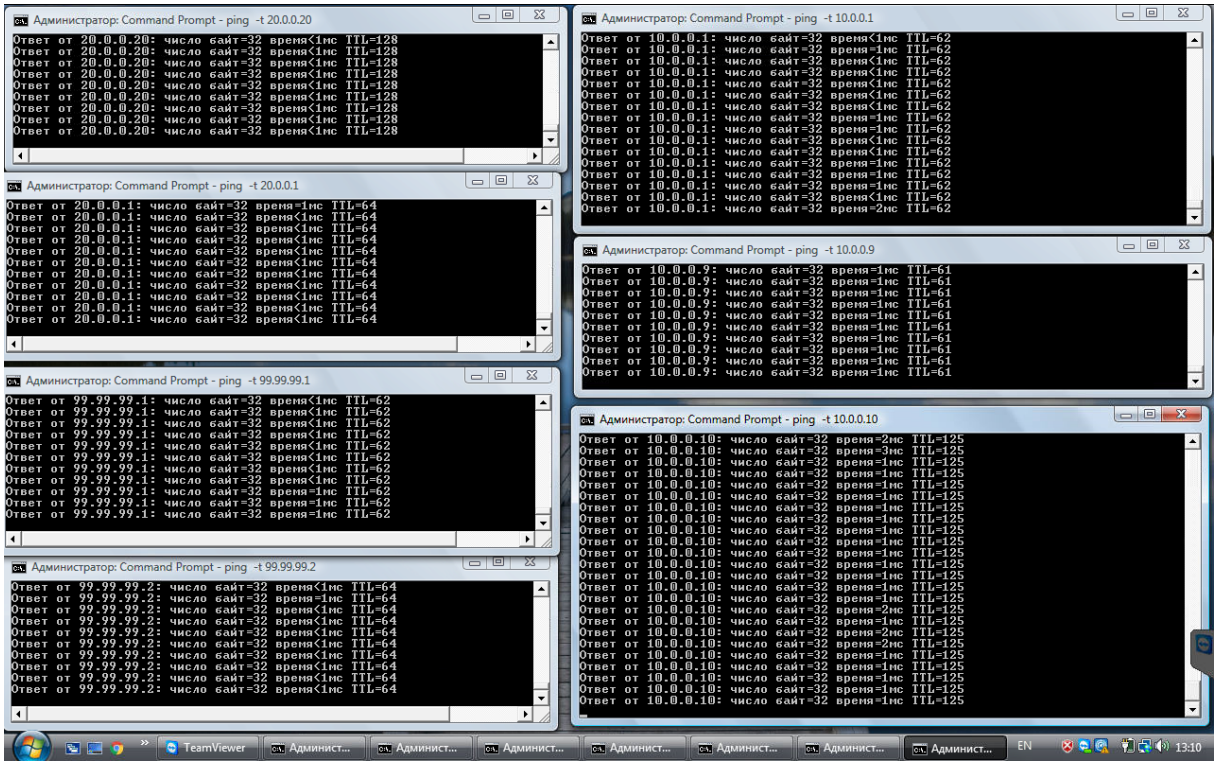
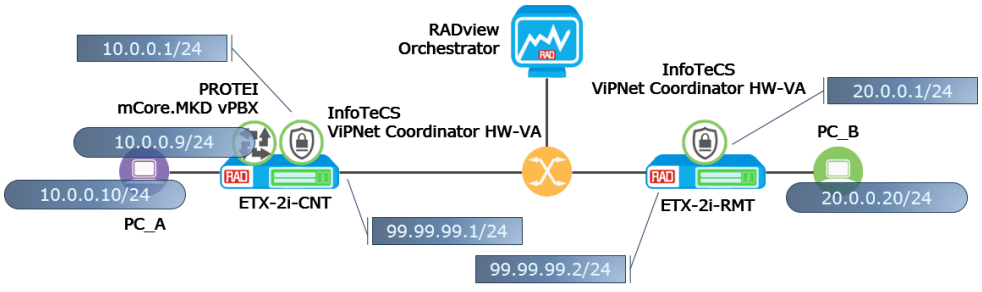


Рисунок 10: Пинги с компьютера PC_B

Этап № 5: Проверка функционала межсетевого экрана (виртуальная функция InfoTeCS ViPNet Coordinator VA)

Цели	Убедиться в правильности работы межсетевого экрана виртуальной функции InfoTeCS ViPNet Coordinator VA
Критерии успеха	Данные, обмен которыми между двумя ПК осуществляется, могут прерываться в зависимости от настроек межсетевого экрана
Схема теста	Схема теста: 

Описание настроек

Для данного теста мы запустим между двумя ПК несколько потоков передачи данных:

- Пинги (см. Рисунок 9: Пинги с компьютера PC_A и Рисунок 10: Пинги с компьютера PC_B)
- Генерация TCP трафика

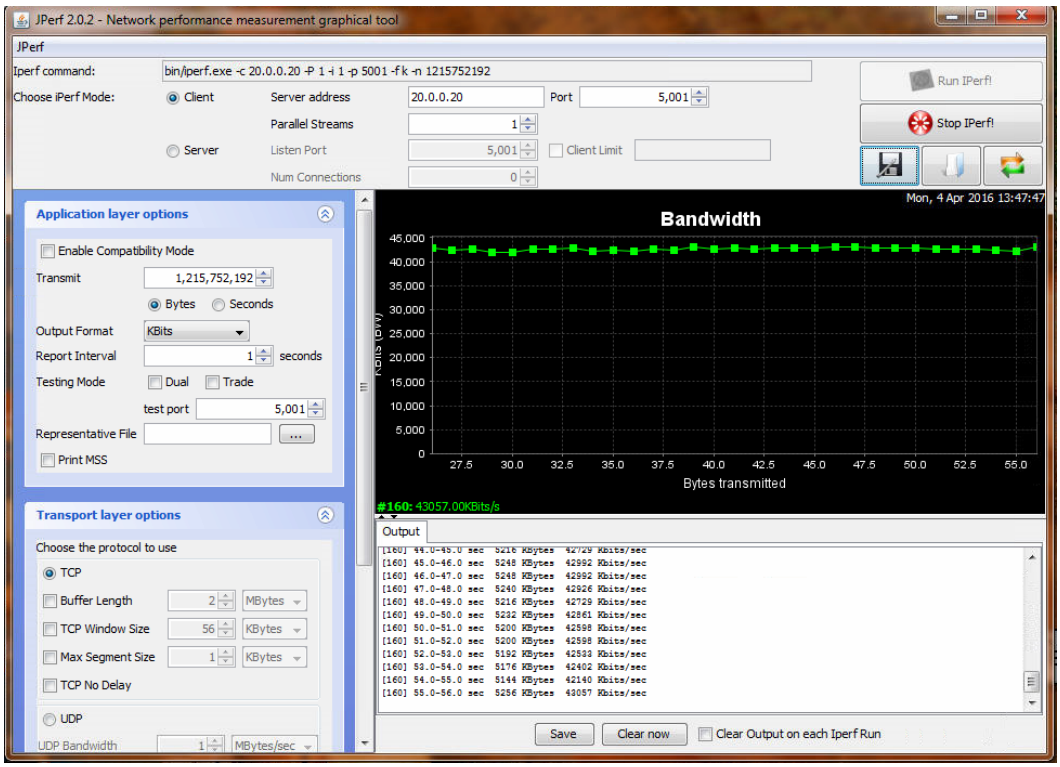


Рисунок 11: Скриншот генератора трафика PC_A (аппаратные возможности ПК не позволяют сгенерировать полосу пропускания более, чем 40 Мб/с)

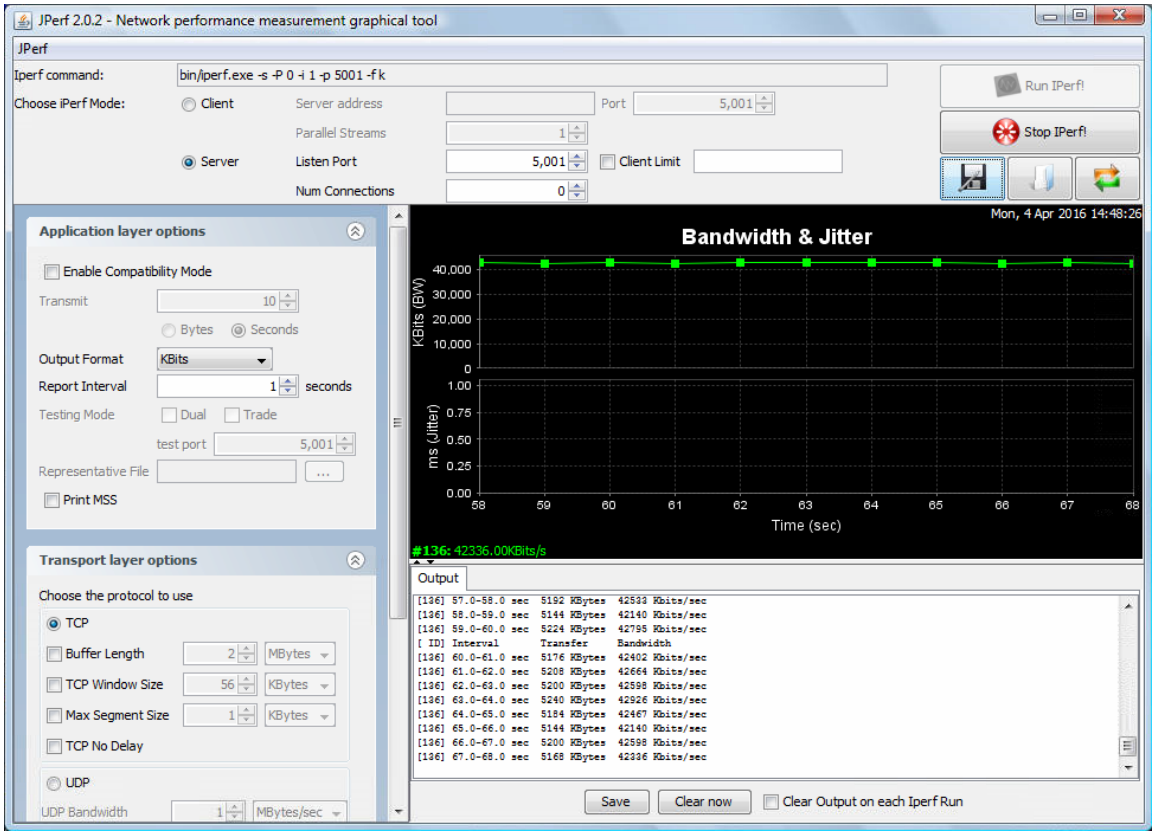
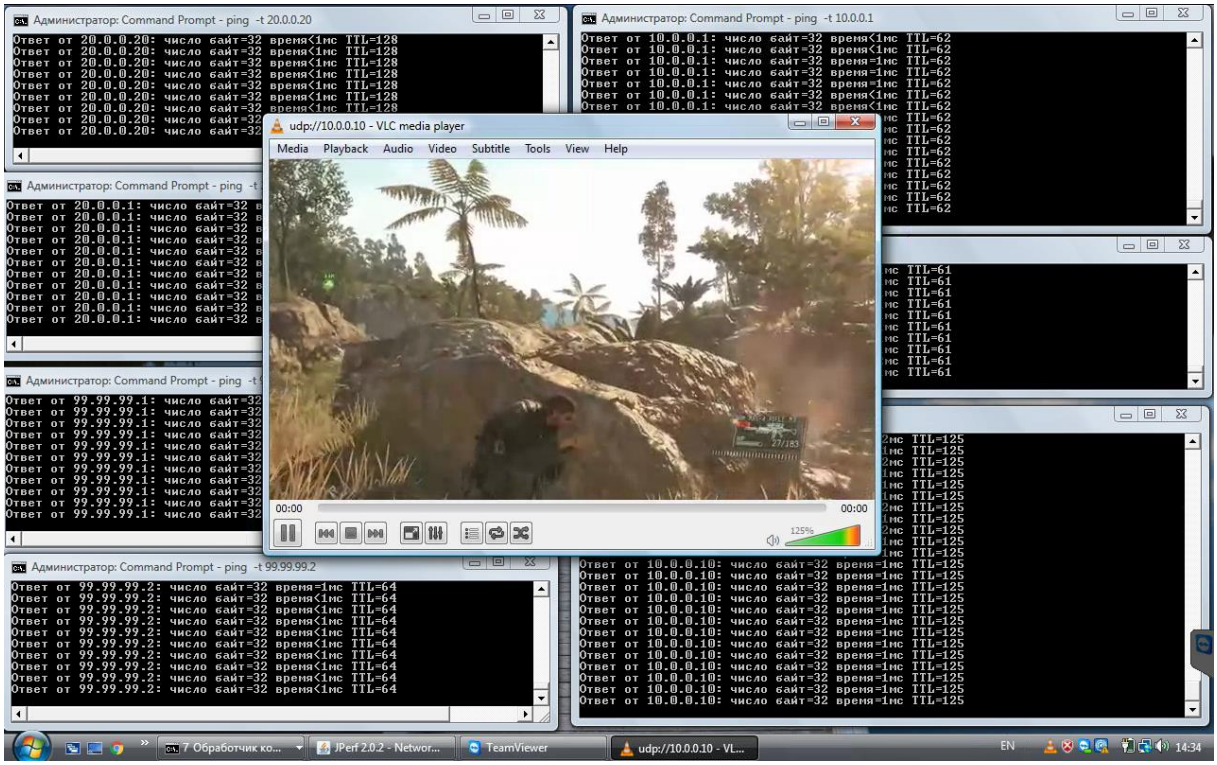


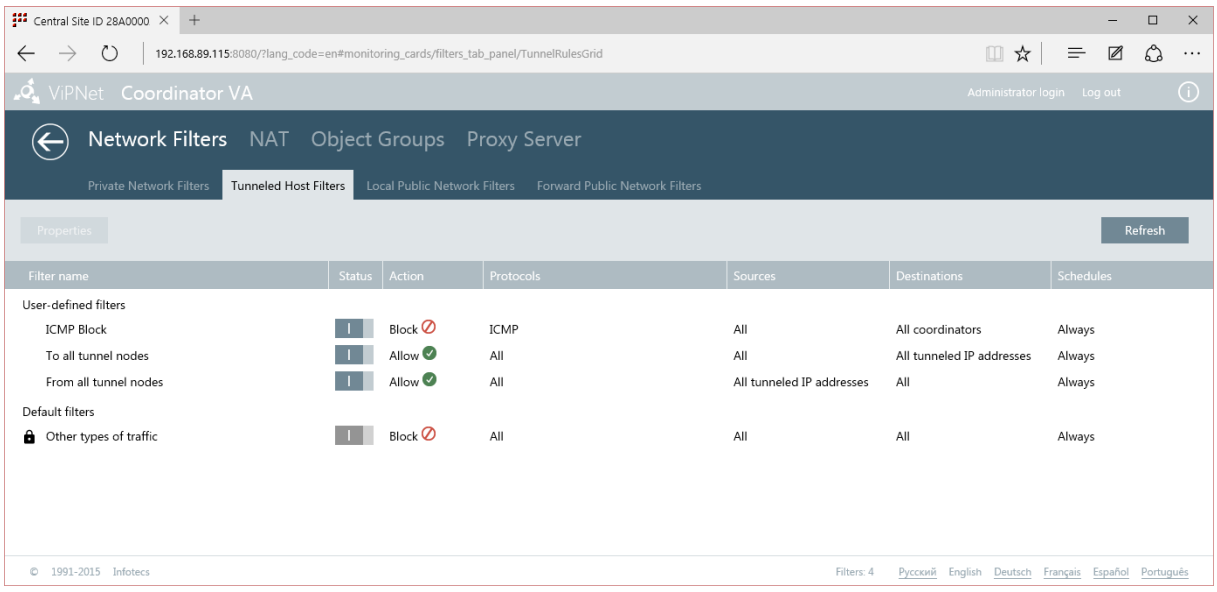
Рисунок 12: Прием трафика на PC_B в объеме равном сгенерированному

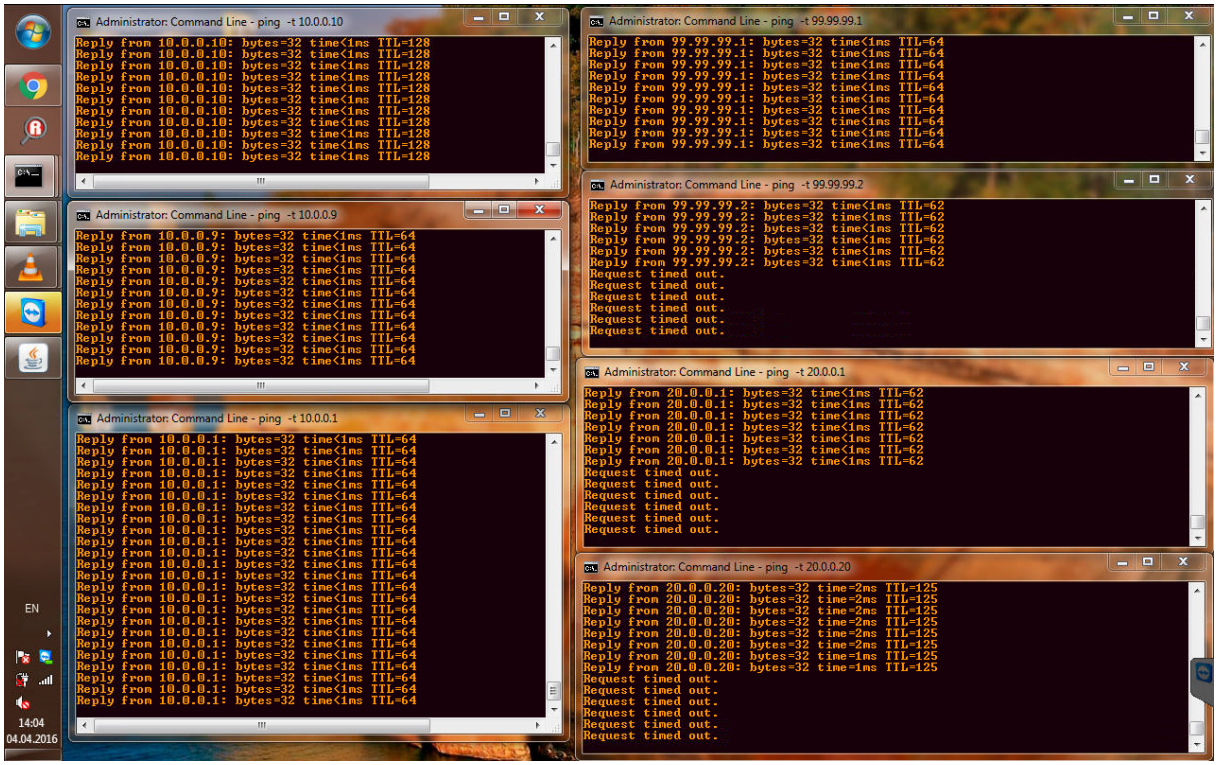
- Передача потокового видео



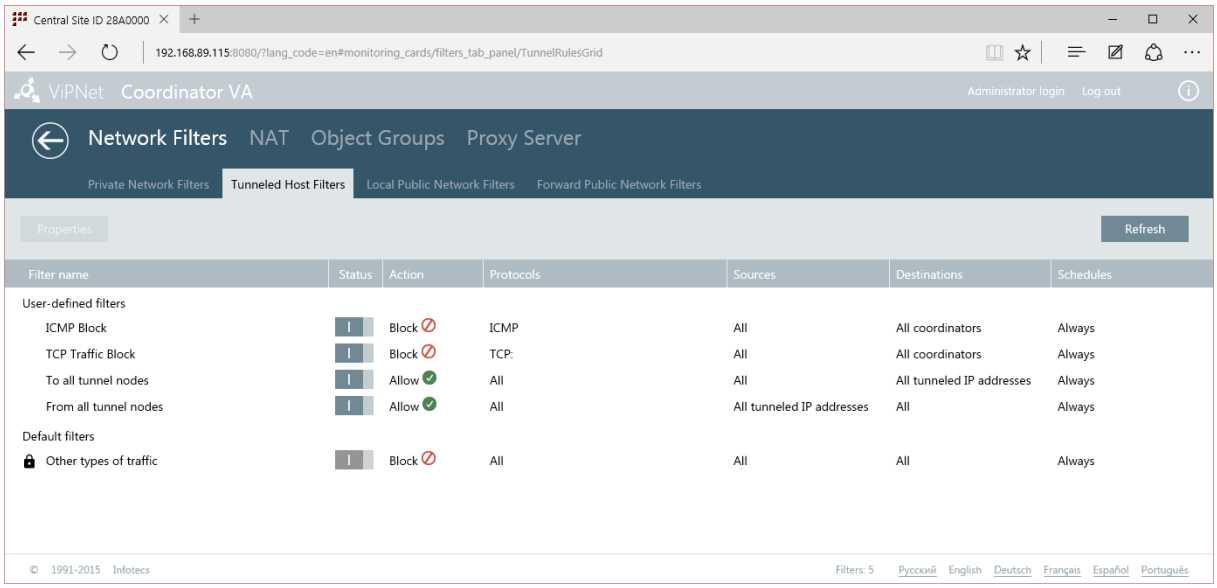
Результат

- Создадим правило, которое запрещает ICMP трафик от PC_A в сторону PC_B – пинги в направлении PC_A – PC_B прервутся

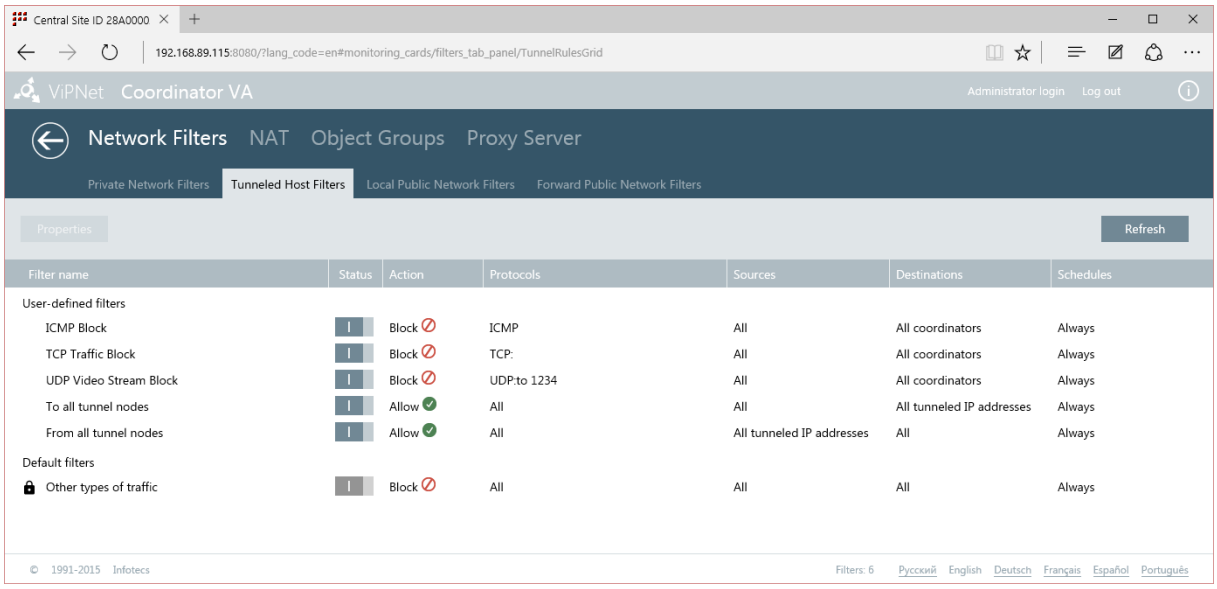




- Создадим правило, которое запрещает TCP трафик от PC_A в сторону PC_B – прием сгенерированного трафика на PC_B прервется

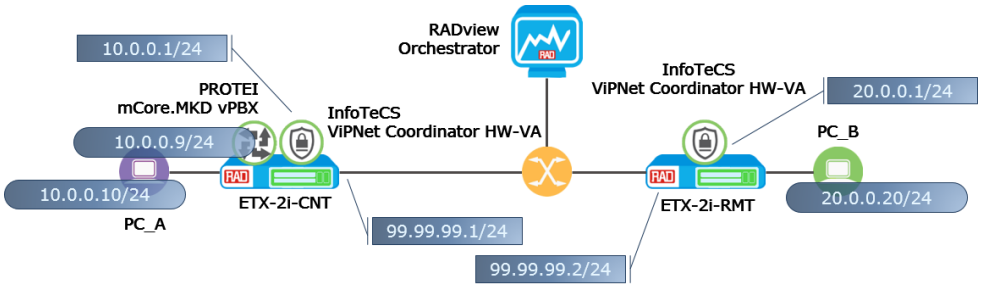


- Создадим правило, которое запрещает UDP трафик на порт 1234 (порт, который слушает PC_B для приема видеовещания) от PC_A в сторону PC_B – прием видеопотока остановится



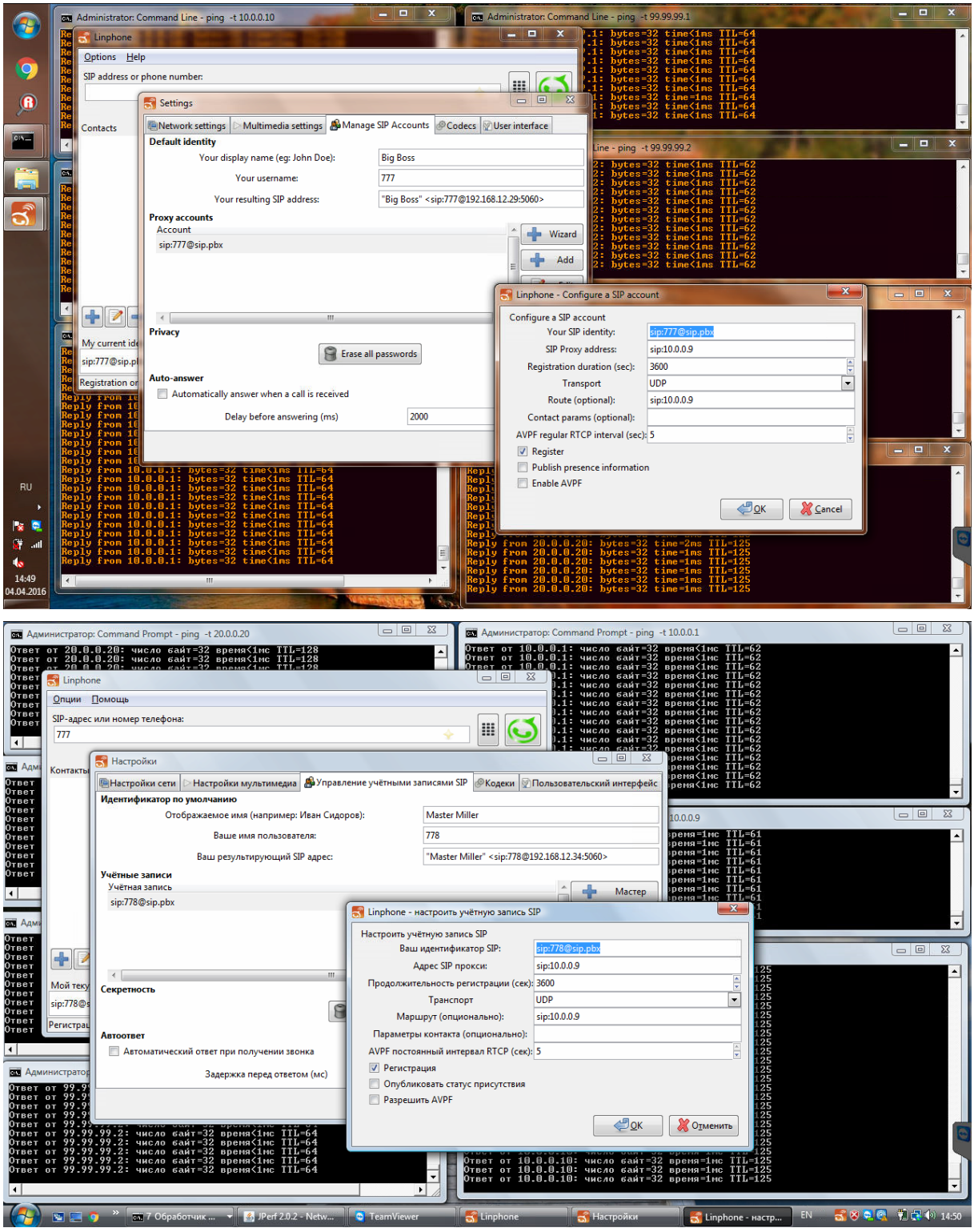
- Для последующих тестов отключим созданные правила фильтрации трафика

Этап № 6: Проверка функционала IP АТС (виртуальная функция PROTEI mCore.MKD vPBX)

Цели	Организовать VoIP звонок между двумя ПК через IP АТС, исполненной в виде виртуальной функции
Критерии успеха	VoIP звонок осуществлен успешно
Схема теста	Схема теста: 

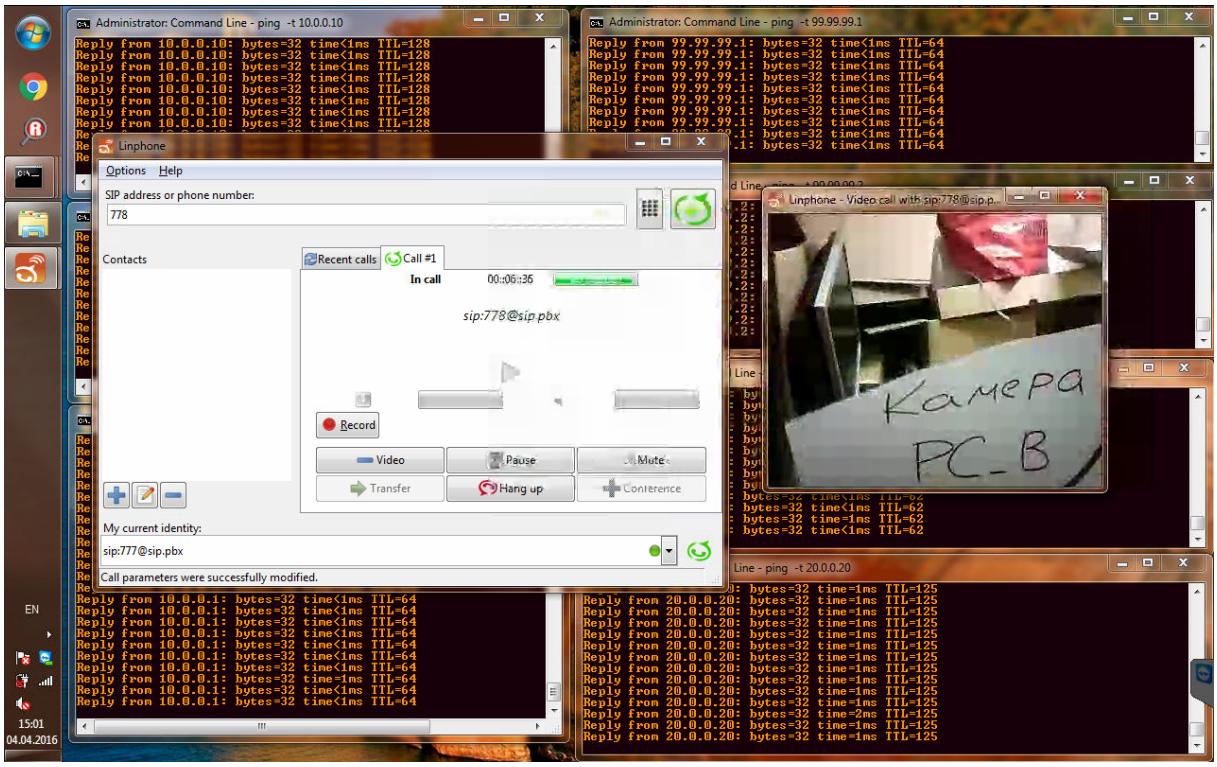
Описание настроек

Ранее мы заранее создали абонентов с номерами 777 и 778 и секретным паролем 111. Теперь введем соответствующие абонентские данные на клиентские ПК:

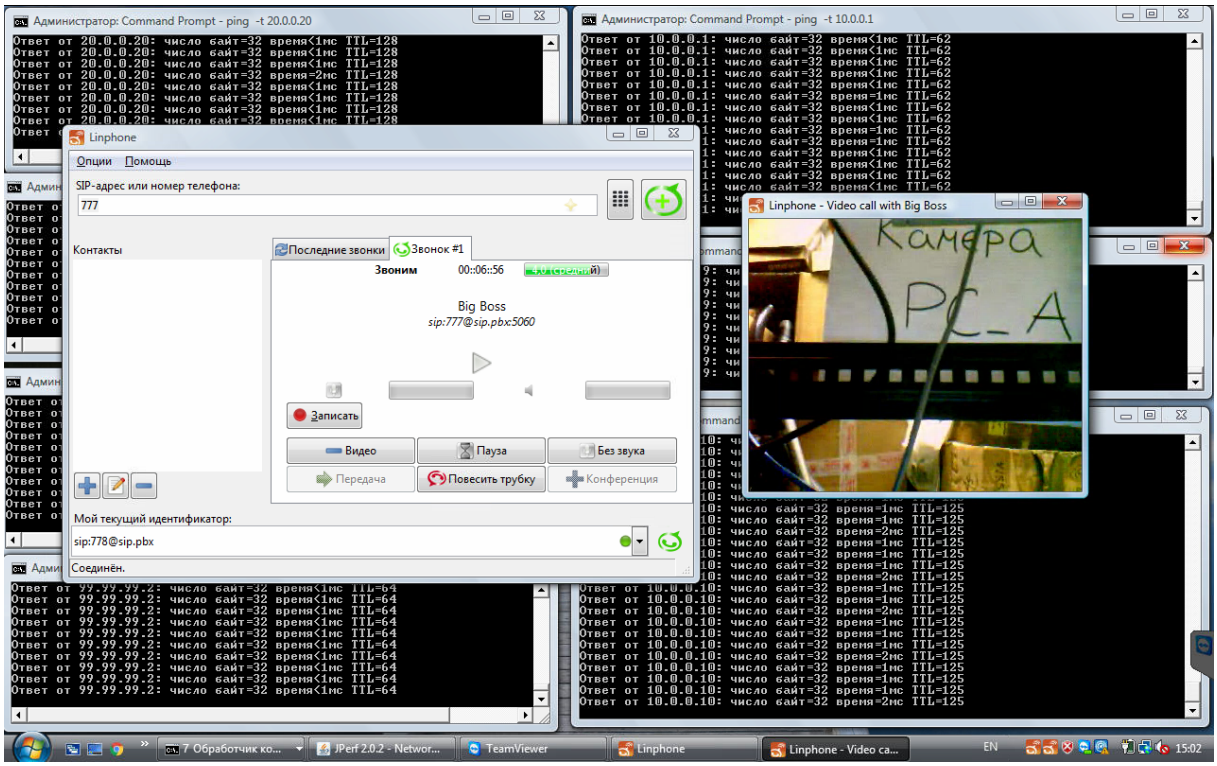

Administrator: Command Line - ping -t 10.0.0.10
Administrator: Command Line - ping -t 99.99.99.1
Linphone
Options Help
SIP address or phone number:
Contacts
Settings
Network settings
Multimedia settings
Manage SIP Accounts
Codecs
User interface
Default identity
Your display name (eg: John Doe):
Big Boss
Your username:
777
Your resulting SIP address:
"Big Boss" <sip:777@192.168.12.29:5060>
Proxy accounts
Account
sip:777@sip.pbx
Wizard
Add
Privacy
Erase all passwords
Auto-answer
Automatically answer when a call is received
Delay before answering (ms)
2000
Linphone - Configure a SIP account
Configure a SIP account
Your SIP identity:
sip:777@sip.pbx
SIP Proxy address:
sip:10.0.0.9
Registration duration (sec):
3600
Transport
UDP
Route (optional):
sip:10.0.0.9
Contact params (optional):
AVPF regular RTCP interval (sec):
5
Register
Publish presence information
Enable AVPF
OK
Cancel
Reply from 10.0.0.1: bytes=32 time<1ms TTL=64
Reply from 20.0.0.20: bytes=32 time=2ms TTL=125
Reply from 20.0.0.20: bytes=32 time=1ms TTL=125
Администратор: Command Prompt - ping -t 20.0.0.20
Администратор: Command Prompt - ping -t 10.0.0.1
Опции Помощь
SIP-адрес или номер телефона:
777
Настройки
Настройки сети
Настройки мультимедиа
Управление учётными записями SIP
Кодеки
Пользовательский интерфейс
Идентификатор по умолчанию
Отображаемое имя (например: Иван Сидоров):
Master Miller
Ваше имя пользователя:
778
Ваш результирующий SIP адрес:
"Master Miller" <sip:778@192.168.12.34:5060>
Учётные записи
Учётная запись
sip:778@sip.pbx
Мастер
Секретность
Автоответ
Автоматический ответ при получении звонка
Задержка перед ответом (мс)
Linphone - настроить учётную запись SIP
Настроить учётную запись SIP
Ваш идентификатор SIP:
sip:778@sip.pbx
Адрес SIP прокси:
sip:10.0.0.9
Продолжительность регистрации (сек):
3600
Транспорт
UDP
Маршрут (опционально):
sip:10.0.0.9
Параметры контакта (опционально):
AVPF постоянный интервал RTCP (сек):
5
Регистрация
Опубликовать статус присутствия
Разрешить AVPF
OK
Отменить
Ответ от 10.0.0.10: число байт=32 время=1мс TTL=125

Результат

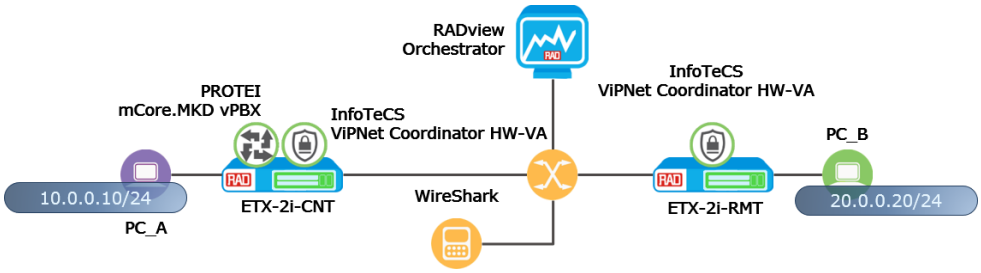
- Прием аудио и видео от PC_B на компьютере PC_A



- Прием аудио и видео от PC_A на компьютере PC_B



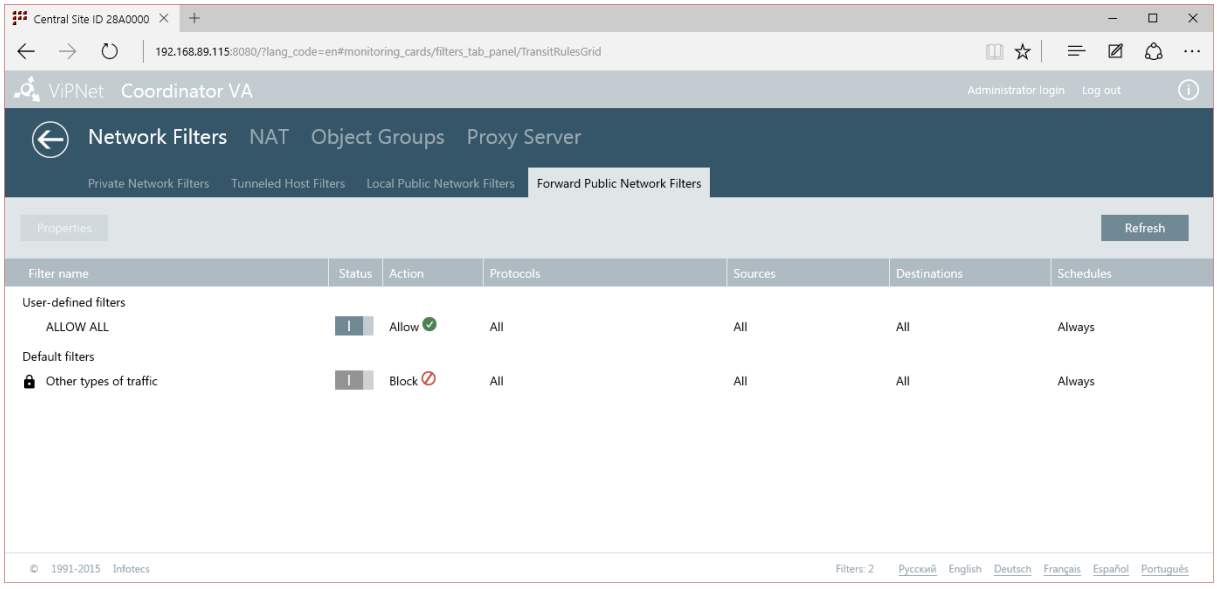
Этап № 7: Проверка шифрования в канале между двумя узлами

Цели	Убедиться в том, что канал между двумя узлами шифрован и информацию из него невозможно перехватить
Критерии успеха	Информацию, переданную от PC_A к PC_B, невозможно перехватить в открытом виде
Схема теста	Схема теста: 

Описание настроек

Для осуществления данного теста мы отключим шифрование на ПО ViPNet Coordinator VA на обоих узлах. Для этого мы закомментируем в конфигурации координатора информацию о туннелировании. Это приведет к тому, что ПО будет функционировать в режиме обычного маршрутизатора с функцией межсетевого экрана.

Также необходимо добавить в разделе «Транзитные фильтры открытой сети» правило по-умолчанию на пропуск любого типа трафика. Данное правило необходимо добавить на обоих виртуальных функциях.



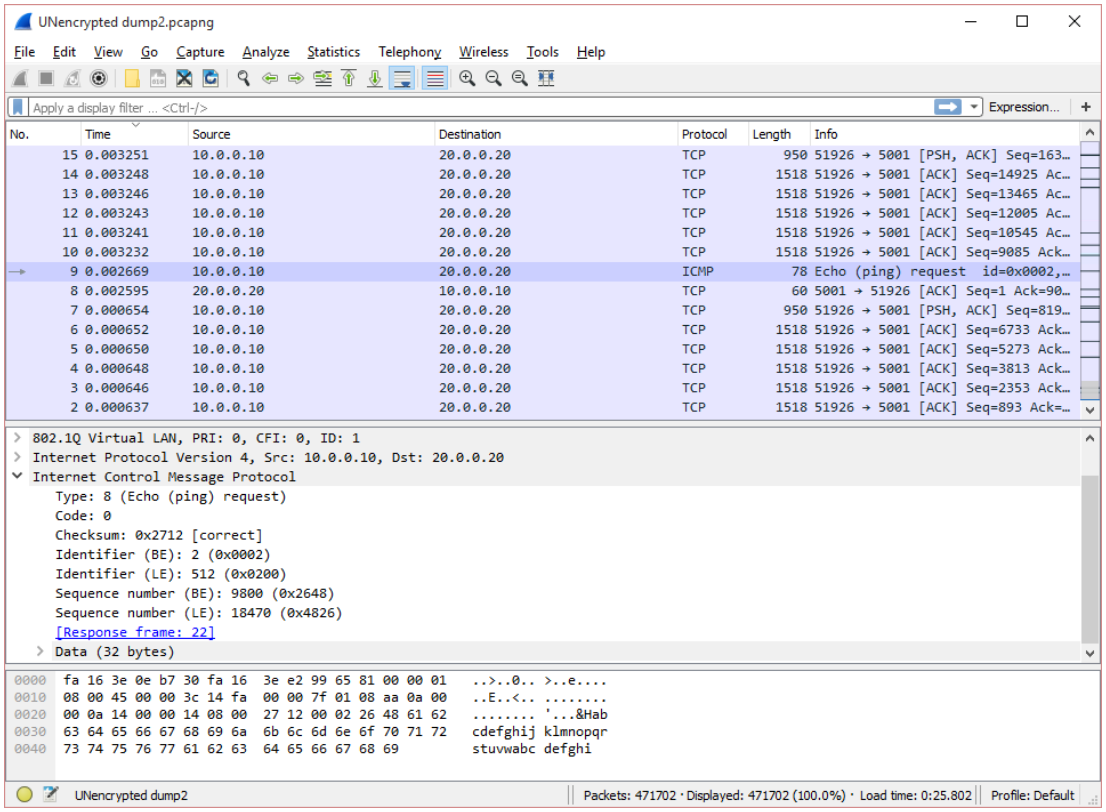
После того, как мы все сделали верно оба компьютера также смогут друг друга пинговать и передавать данные, но осуществляться это будет по незашифрованному каналу.

К промежуточному коммутатору, соединяющему оба устройства мы подключим сниффер WireShark, а на самом коммутаторе настроим зеркалирование трафика с клиентского канала, дабы можно было перехватывать все клиентские данные.

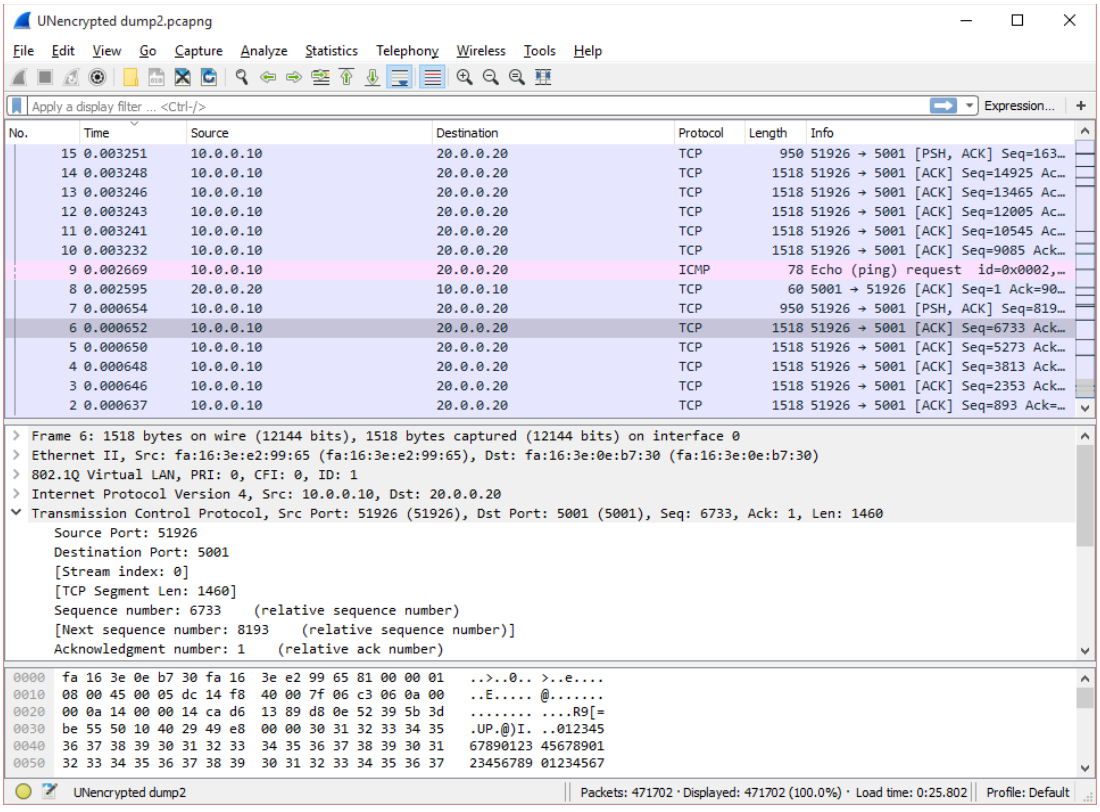
Результат

В существующей конфигурации запустим сниффер и проанализируем полученные данные:

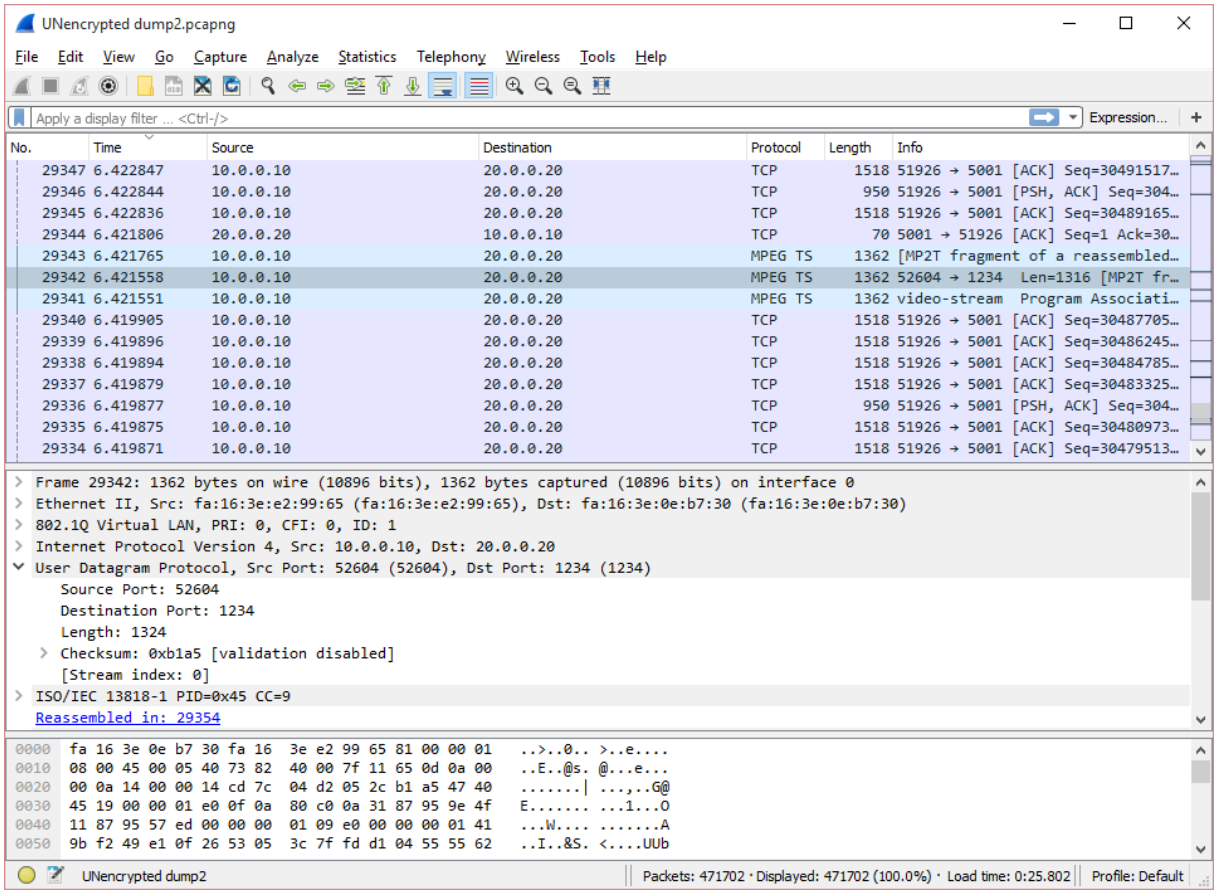
- Видны пинги



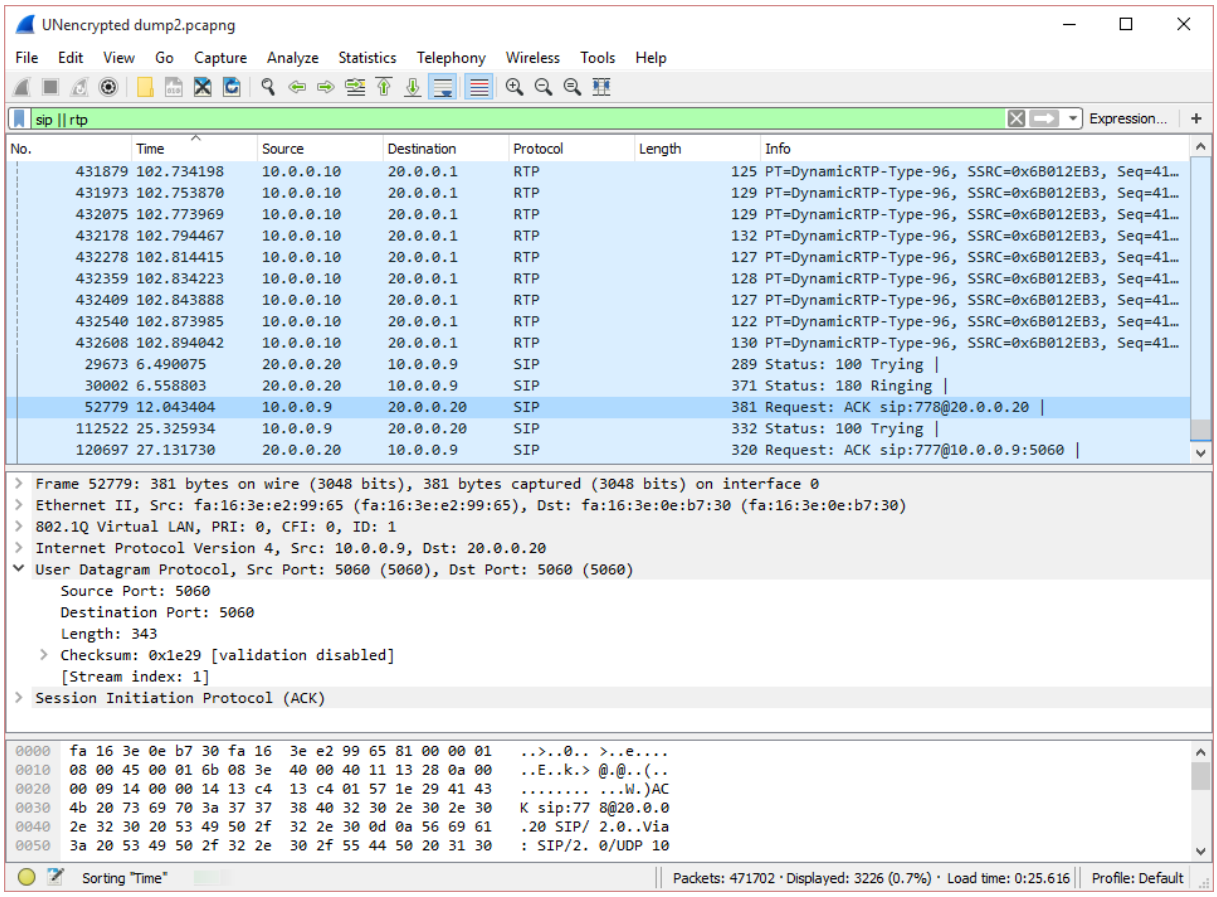
- Видна передача данных посредством протокола TCP

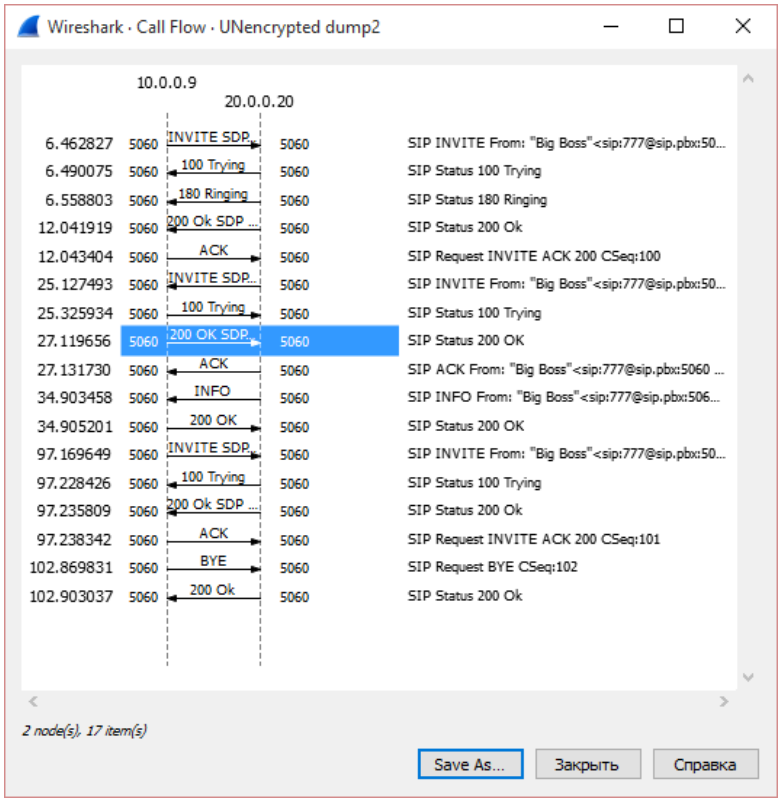


- Видна трансляция видеопотока

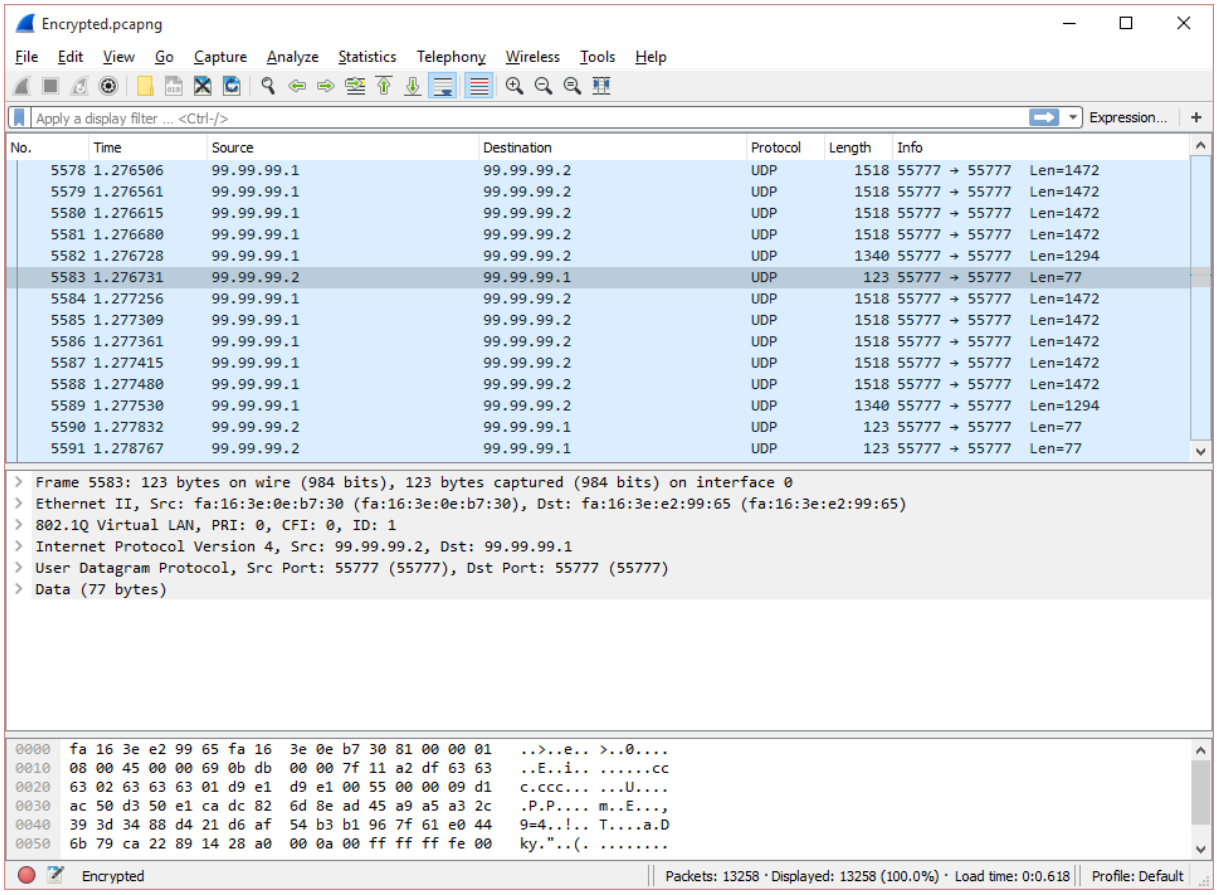


- Виден VoIP звонок



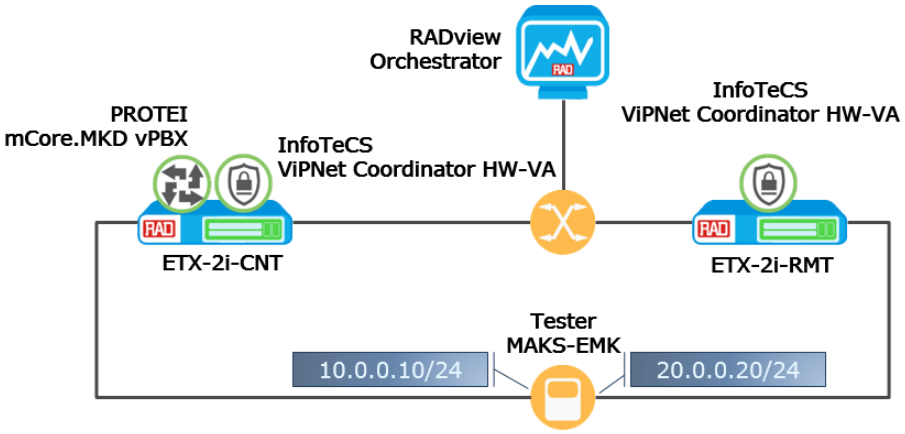


Посмотрим тот же трафик, но с включенным шифрованием.



Все, что может отразить сниффер – это UDP трафик между сетевыми интерфейсами ПО ViPNet Coordinator VA, скрывая IP адреса, протоколы и содержимое пакетов клиентской сети.

Этап № 8: Проверка полосы пропускания

Цели	Проверить производительность клиентского канала, проложенного через виртуальные функции
Критерии успеха	Измерительное устройство успешно передает и принимает сгенерированные данные через клиентский канал связи
Схема теста	Схема теста: 

Описание настроек

Прежде, чем мы осуществим нагрузочный тест через клиентский канал связи, проведем его через аналогичный канал, но без виртуальных функций для того, чтобы убедиться, что физическое оборудование не вносит существенного вклада в передаваемый поток данных.

Для этого мы используем клиентские порты Ethernet 0/4 на оборудовании ETX-2i. Клиентский траффик будет приходить нетегированным, тегироваться VLAN'ом 200 и передаваться далее в сеть. Конфигурация обоих ETX-2i будет выглядеть следующим образом:

```
configure flows
classifier-profile "class_novnf" match-any
match vlan 200
exit all

configure flows
classifier-profile "class_untagged" match-any
match untagged
exit all

configure flows
flow "novnf_eth4_eth1"
classifier "class_untagged"
vlan-tag push vlan 200 p-bit fixed 5
ingress-port ethernet 0/4
```

```
egress-port ethernet 0/1 queue 0 block 0/1
no shutdown
exit all

configure flows
flow "novnf_eth1_eth4"
policer profile "Policer1"
vlan-tag pop vlan
ingress-port ethernet 0/1
egress-port ethernet 0/4 queue 0 block 0/1
no shutdown
exit all
```

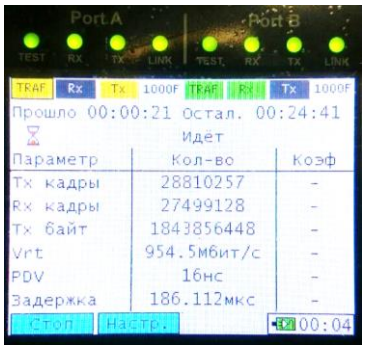
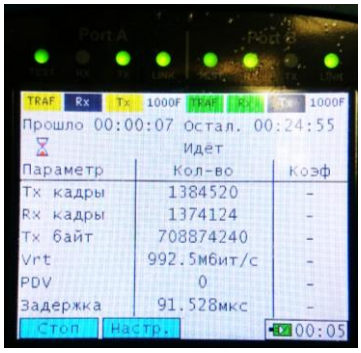
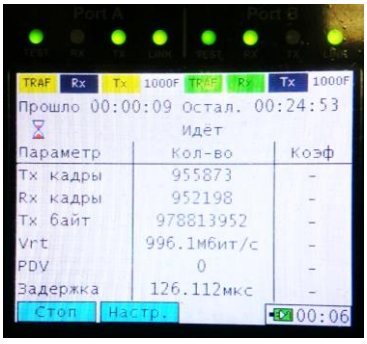
В качестве измерительного устройства мы будем использовать тестер-анализатор пакетных сетей МАКС-ЕМК, производства компании КОМЕТЕХ.

Тестер-анализатор пакетных сетей МАКС ЕМК предназначен для количественной оценки параметров качества, диагностики современных систем связи на основе технологии IP, выполнения измерений параметров сетей передачи данных, для контроля их на соответствие регламентированному уровню качества предоставления услуг. Прибор также позволяет измерять параметры качества синхронизации различных систем с измерением расхождение шкал времени в сетях операторов связи.

Контроль параметров транспортных потоков сетей Ethernet, Fast Ethernet и Gigabit Ethernet проводится в соответствии с международными рекомендациями.

Рисунок 13: Тестер-анализатор пакетных сетей МАКС-ЕМК

Ниже приведены результаты измерений:

Размер пакета, Б	Состояние теста	Статистика измерений
64		
256		
512		
1024		

Данные измерения позволят нам сформировать базисную линию для дальнейшего проведения теста.

Результат

Протестируем канал связи через виртуальные функции, собирая информацию не только с тестера, но используя статистику устройств ETX-2i. В качестве контролируемого

потока данных мы возьмем исходящий поток с x86 модуля на клиентский порт ETX-2i-RMT, то есть тот поток, что прошел полностью через клиентский канал.

Прежде чем снимать данные с выбранного потока, посмотрим статистику потока данных до виртуальных функций и клиентского канала (выдержка из выведения статистики):

```
ETX-2i-CNT-RTR>config>flows>flow(vnf_v1_p3_p7)# show statistics running

Peak Measurement
------------------------------------------------------------------------------
                        L1 Min        L2 Min        L1 Max        L2 Max
Tx Bit Rate [bps]    : 1021772120    726920760     1022625448    727774088
Drop Bit Rate [bps] : 45435648      34617728      48704032      34663072
```

Мы видим, что в канал входит поток данных с полосой пропускания в 1 Гб/с.

Ниже приведем статистику итогового потока:

- Длина пакета: 64 Байт
  - Показания тестера

  - Статистика потока ETX-2i-RMT

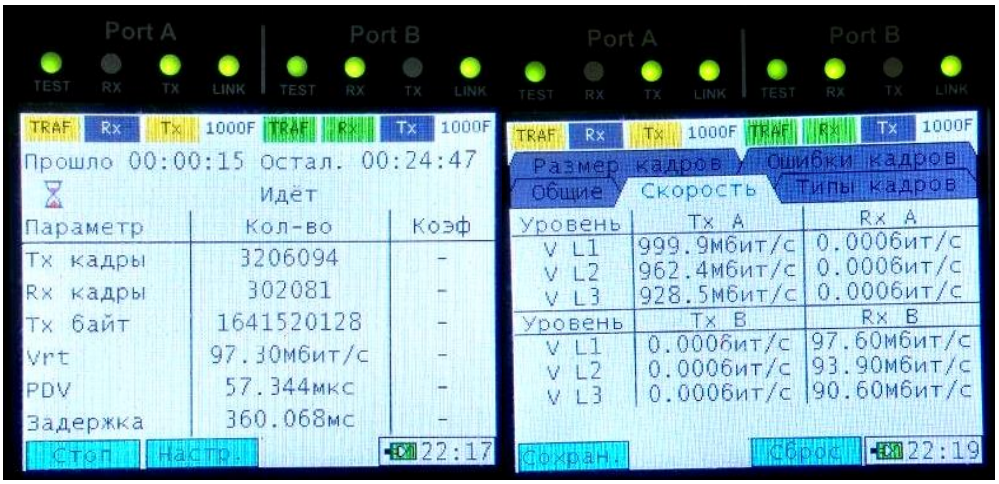
```
ETX-2i-RMT>config>flows>flow(vnf_v1_p7_p3)# show statistics running
Peak Measurement
------------------------------------------------------------------------------
                        L1 Min        L2 Min        L1 Max        L2 Max
Tx Bit Rate [bps]    : 42611688      32701288      42613136      32702736
Drop Bit Rate [bps] : 0             0             0             0
```

- Длина пакета: 256 Байт
  - Показания тестера

- Статистика потока ETX-2i-RMT

```
ETX-2i-RMT>config>flows>flow(vnf_v1_p7_p3)# show statistics running
Peak Measurement
-------------------------------------------------------------------------------
                          L1 Min          L2 Min          L1 Max          L2 Max
Tx Bit Rate [bps]    : 81803728        75951888        81925760        76073920
Drop Bit Rate [bps] : 0               0               0               0
```

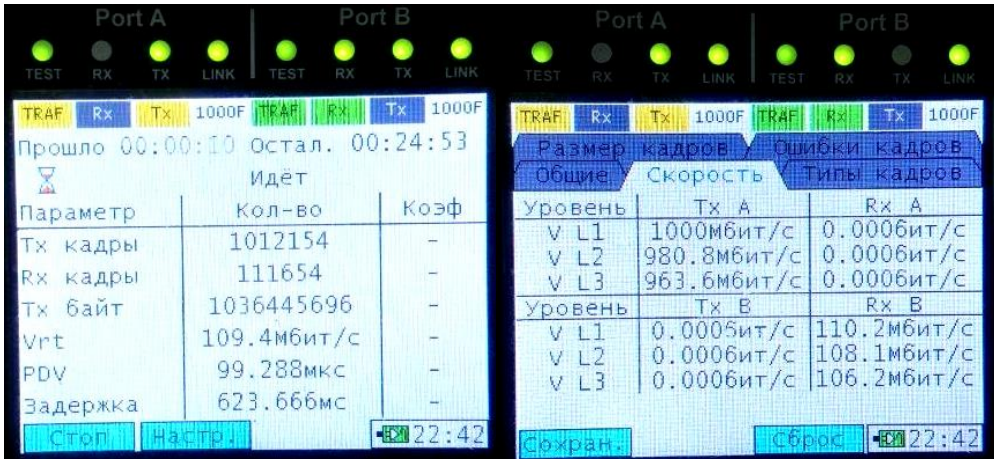
- Длина пакета: 512 Байт
  - Показания тестера



  - Статистика потока ETX-2i-RMT

```
ETX-2i-RMT>config>flows>flow(vnf_v1_p7_p3)# show statistics running
Peak Measurement
-------------------------------------------------------------------------------
                          L1 Min          L2 Min          L1 Max          L2 Max
Tx Bit Rate [bps]    : 99793464        94866424        99793464        94866424
Drop Bit Rate [bps] : 0               0               0               0
```

- Длина пакета: 1024 Байт
  - Показания тестера



  - Статистика потока ETX-2i-RMT

```
ETX-2i-RMT>config>flows>flow(vnf_v1_p7_p3)# show statistics running
Peak Measurement
-------------------------------------------------------------------------------
                          L1 Min          L2 Min          L1 Max          L2 Max
Tx Bit Rate [bps]    : 110049728       107833088       110828264       108611624
Drop Bit Rate [bps] : 0               0               0               0
```

Итоговые значения производительности сведем в таблицу:

Размер пакета, Б	Полоса пропускания
64	40,3 Мб/с
256	83,5 Мб/с
512	97,3 Мб/с
1024	110,2 Мб/с

Необходимо заметить, что полученные показатели производительности укладываются в рамках ожидаемого, поскольку определяются производительностью шифрования виртуальной функции ИнфоТеКС. Для увеличения скорости шифрования необходимо большее выделение ресурсов под виртуальную машину (напр., два ядра процессора и более).

5. Заключение

Проведенное тестирование отображает функционирование решения виртуализации сетевых функций на базе платформы ETX. Система оркестрации позволит быстро создать и настроить виртуальную машину на x86 платформе, развернув на ней соответствующее ПО. Это позволяет сделать вывод о том, что данное решение можно применять в ситуациях, когда необходимо развернуть не просто сетевое устройство, но обладающее добавочным функционалом, например, для развертывания на сети абонента IP-АТС/SBC средней емкости или организации шифрованного канала. При этом ETX-2i, обладая стандартным функционалом демаркационного устройства, позволит осуществлять приоритизацию клиентских данных, управление полосой пропускания, измерения качественных показателей клиентского сервиса и нагрузочные тесты для ввода канала в эксплуатацию или диагностики. Управление и конфигурация может осуществляться автоматически удаленно с помощью системы управления RADview, сокращая при этом время на ввод в эксплуатацию услуги, количество выездов специалистов на инсталляцию и время реагирования на аварийные ситуации. Все это позволит расширить портфолио, оказываемых оператором услуг связи и, как результат, увеличить прибыль и сократить совокупную стоимость владения.