

Переход от «исторических» сетей к структурированным

Или как победить зоопарк в инфраструктуре

Быстров Денис
Максофт

192@168.su

ТОП-25

в рейтинге
региональных
IT-компаний

ТОП-100

в рейтинге
российских
IT-компаний

12 лет на рынке IT

1 млрд Годовая выручка

2 офиса Москва, Пенза

112 сотрудников



Олимпиада
Сочи 2014



FIFA WORLD CUP
RUSSIA 2018

Кубок Конфедераций 2017
ЧМ по футболу 2018



Проект «Школа Росатома»
4 региона



Оснащение перинатальных
центров 2017-2018
12 регионов

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ



РОСАТОМ



НО РАО



БИЛИБИНО



НИКИРЗ



СМОЛЕНСК



Ростех



КАПШАЙ



НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ
«РУБИН»



БАНК
КУЗНЕЦКИЙ



РОСНЕФТЬ
ТОПЛИВНЫЕ КАРТЫ



ГАЗПРОМ



РВД



ЭЛЕКТРОГЕНЕРАЦИЯ
ИНТЕР РАО



МАГНИТ



Правительство
Пензенской
Области



Министерство образования
Пензенской области



ТНС ЭНЕРГО



КОНТАКТЫ

ПЕНЗА

+7 (8412) 34-34-34
info@maksoft.ru
ул. Куйбышева, д. 28

МОСКВА

+7 (495) 139-36-85
info@maksoft.ru
г. Москва, проспект Мира д.40 офис №814



Сети с «историческим» развитием

- вызывают истерические реакции

- Инфраструктура заказчика росла по мере роста потребностей компании
- Изначально использовалось недорогое домашнее оборудование
- С увеличением числа сотрудников просто докупалось такое же
- ЛВС нам сторож по ночам прокладывал – он в армии телефонистом был
- «Сын главбуха» посоветовал крутую железяку, но настраивать некому и она не работает
- Открылся филиал, у нас теперь по RDP все работает (даже SIP)

Заметки в полях

- Вообще-то я не специалист по этим гравицаппам...

У нас был интернет 10 мбит/с и все быстро работало, а потом мы перешли на 50 мбит/с, но скорость стала только 30 мбит/с – скажите это нас провайдер так обманывает?

(003 - rid)

Почему на выходных, когда работает «Вася», Wi-fi бежит быстро, а когда я прихожу – все страшно тупит?

(еланак ан апутсод кечот 51)

Нам нужно объединить два офиса по VPN, в одном офисе у нас *(*)-Link, а в другом K/n2,7tic II. Еще у нас ГлавБух из дома хочет работать и public ip адреса в офисах динамические. Сделаете?

(тен онченок)

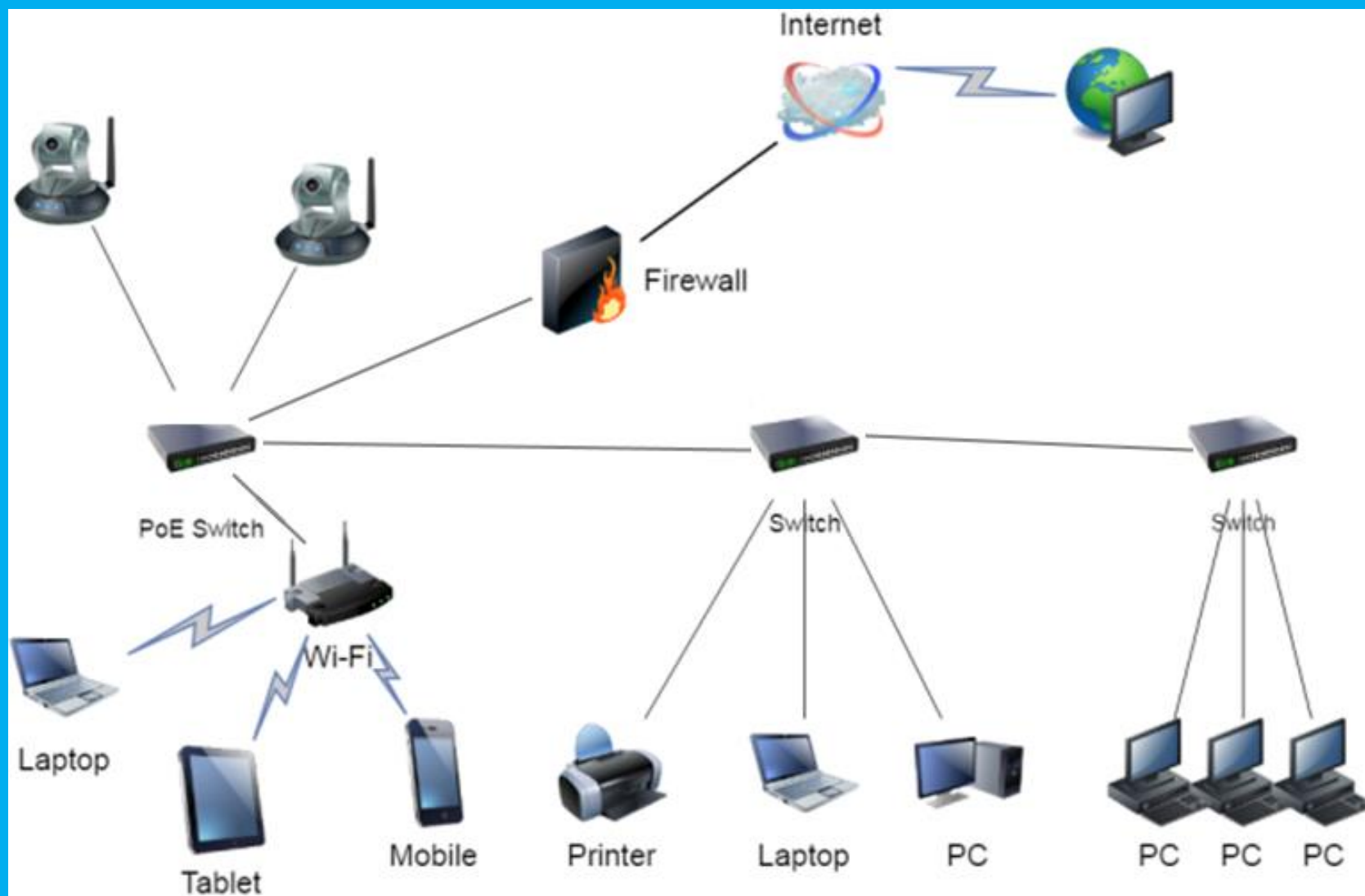
Почему у нас SIP-телефония квакает и Скайп отваливается во время разговоров, у нас же интернет 50 мбит/с?

(акиндуртос акубтуон с ытнеррот)

Почему у нас база 1С грузится 5 минут, а в комнате через коридор меньше минуты?

(йечтивс зи аднялриг)

Сферическая сеть в вакууме



RB-2011 как роутер и свитч ядра

Почему так не нужно делать

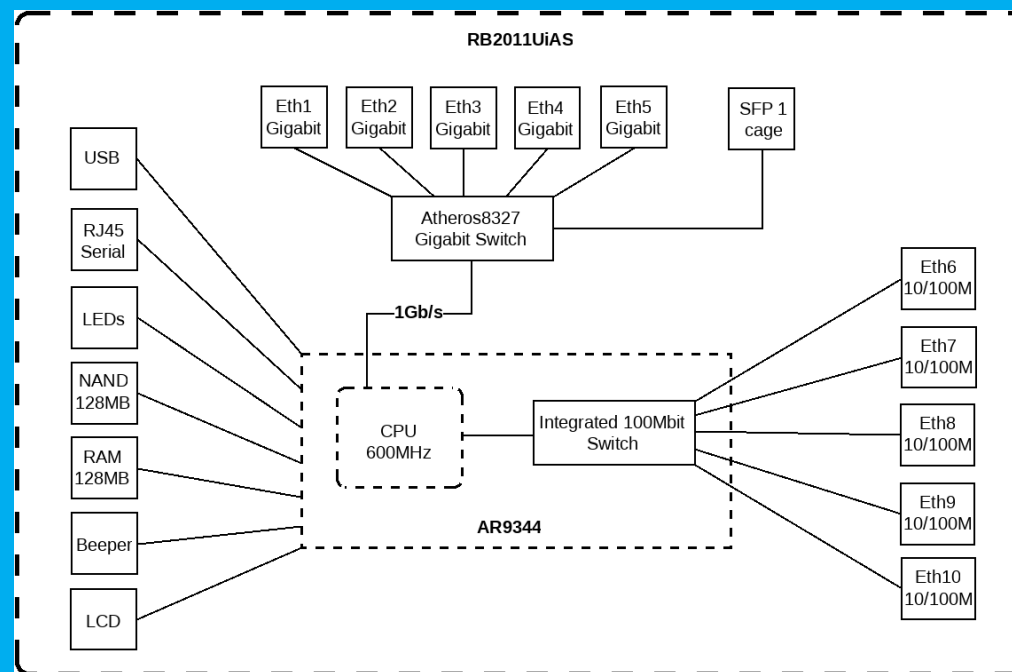
- *Роутер ≠ L3 Свитч*

Почему так можно делать

- ➔ ➔ ➔

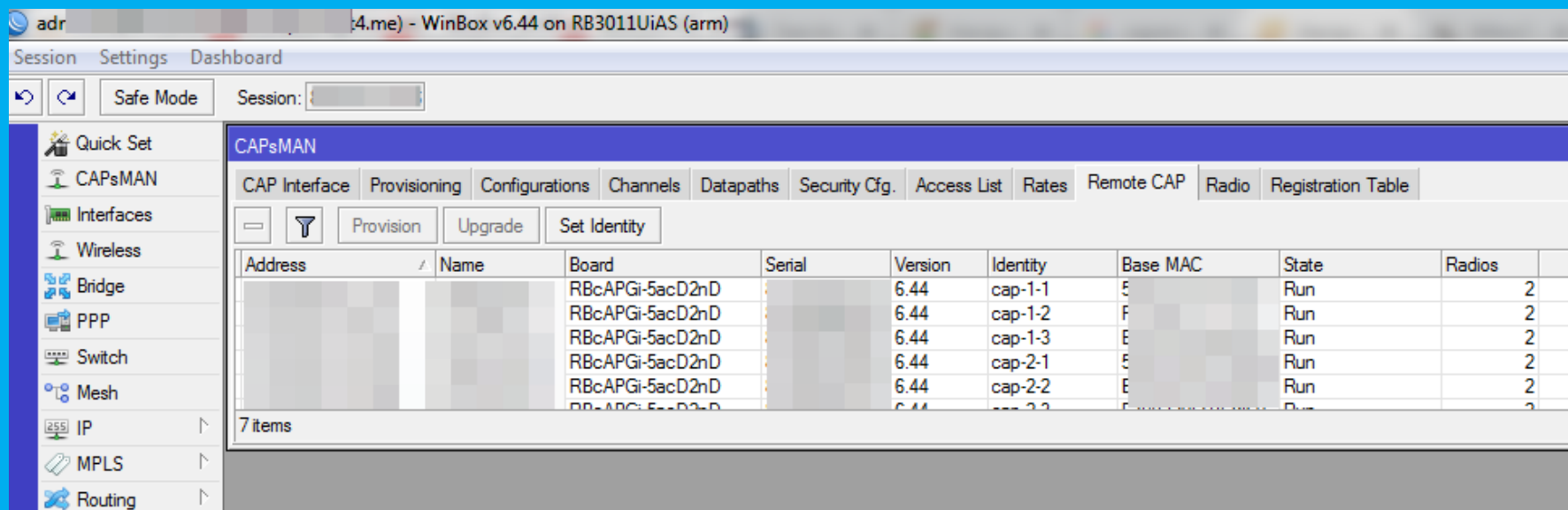
Почему так нужно делать

- Контроль
- Управление
- Мониторинг



CAPsMAN

- Быстро разворачивается
- Централизованно управляется
- Легко обновляется



VPN в каждый офис

- Объединение офисов
- Подключение удаленных/надомных сотрудников
- Предоставление привычных сервисов сотрудникам в командировках

Защита от подбора паролей

Быстро избавиться от непрошенных гостей

Firewall									
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
+ - ✓ ✗ 📁 🏠 ⏏ Reset Counters ⏏ Reset All Counters									
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Connection State	Src. Address List
::: rdp bruteforce - reject									
18	✗ drop	forward			6 (tcp)		3389	new	bf_rdp_st4
::: rdp bruteforce - stage 4									
19	➡ add src to address list	forward			6 (tcp)		3389	new	bf_rdp_st3
::: rdp bruteforce - stage 3									
20	➡ add src to address list	forward			6 (tcp)		3389	new	bf_rdp_st2
::: rdp bruteforce - stage 2									
21	➡ add src to address list	forward			6 (tcp)		3389	new	bf_rdp_st1
::: rdp bruteforce - stage 1									
22	➡ add src to address list	forward	1192.168.17.0/24		6 (tcp)		3389	new	

Свойства системы

Имя компьютера Оборудование

Дополнительно Защита системы Удаленный доступ

Удаленный помощник

☒ Разрешить подключения удаленного помощника к этому компьютеру

[Что происходит при включении удаленного помощника?](#)

Дополнительно...

Удаленный рабочий стол

Выберите вариант и укажите, кому разрешено подключение.

☐ Не разрешать удаленные подключения к этому компьютеру

☒ Разрешить удаленные подключения к этому компьютеру

☒ Разрешить подключения только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети (рекомендуется)

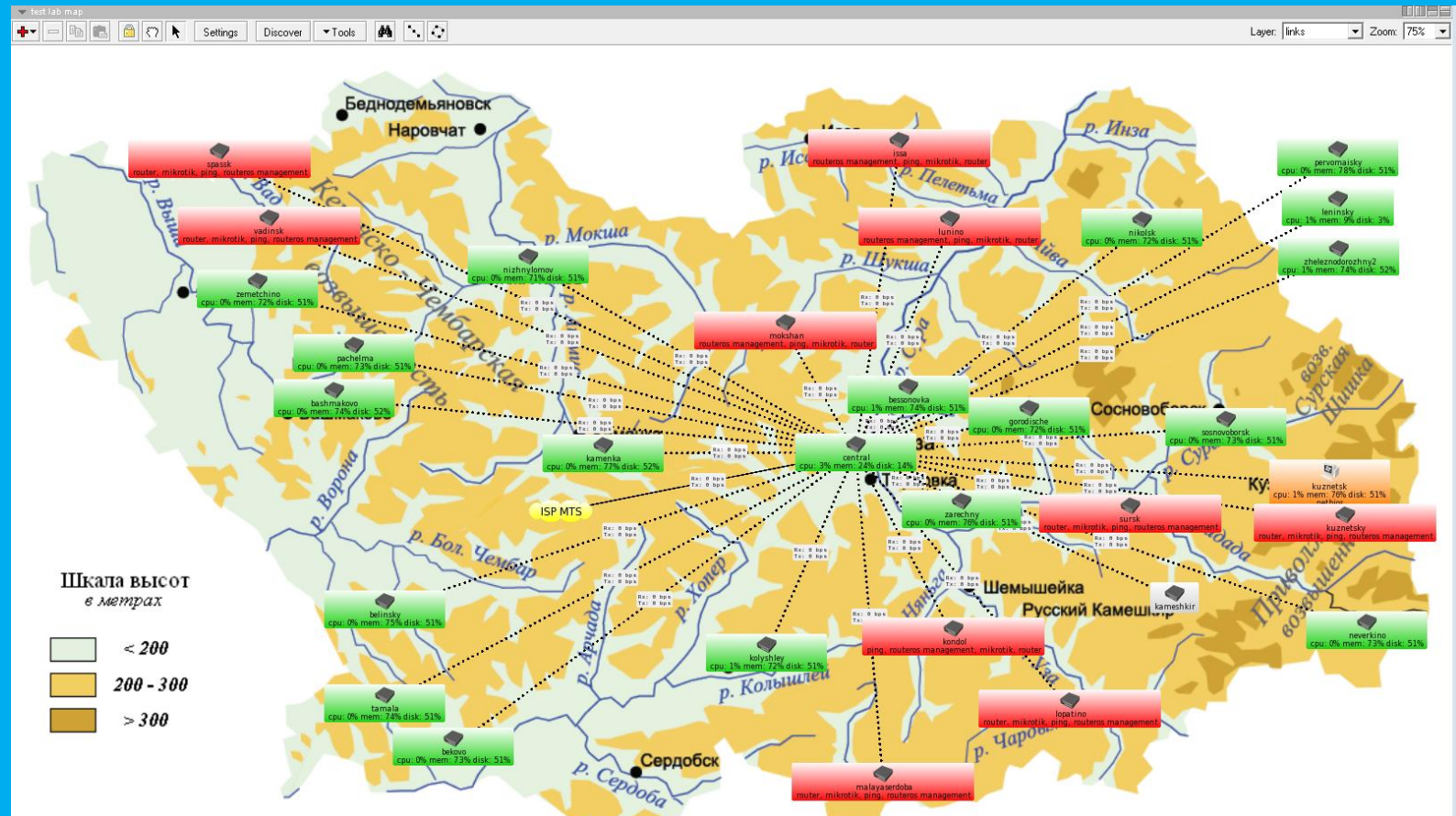
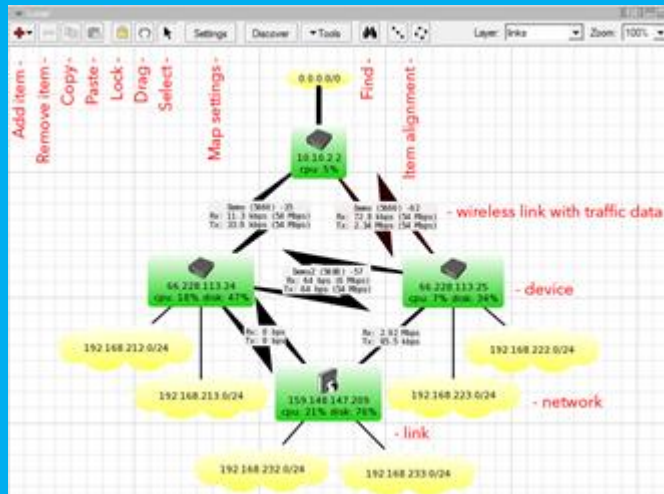
[Помочь выбрать](#) [Выбрать пользователей...](#)

OK Отмена Применить

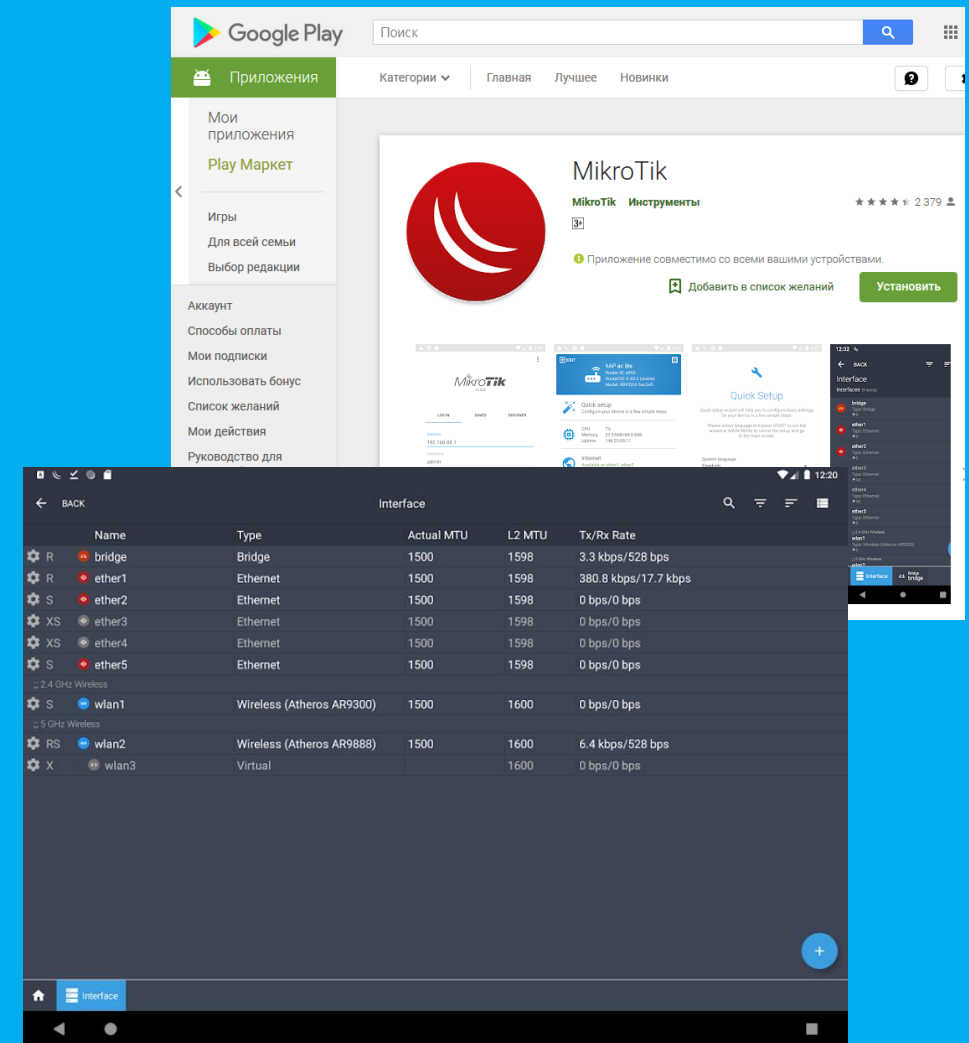
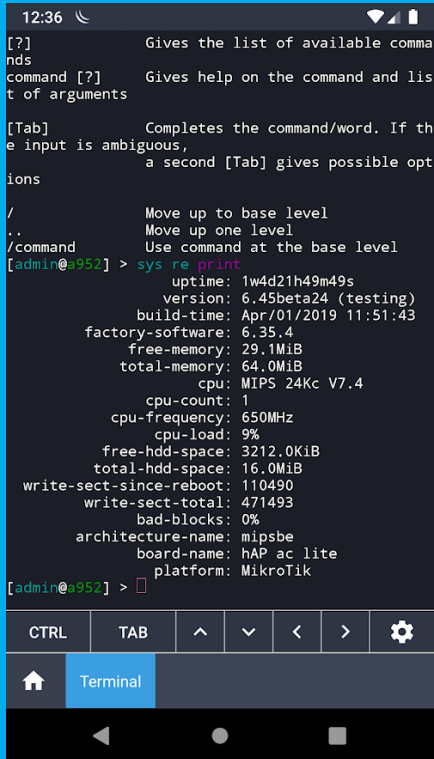
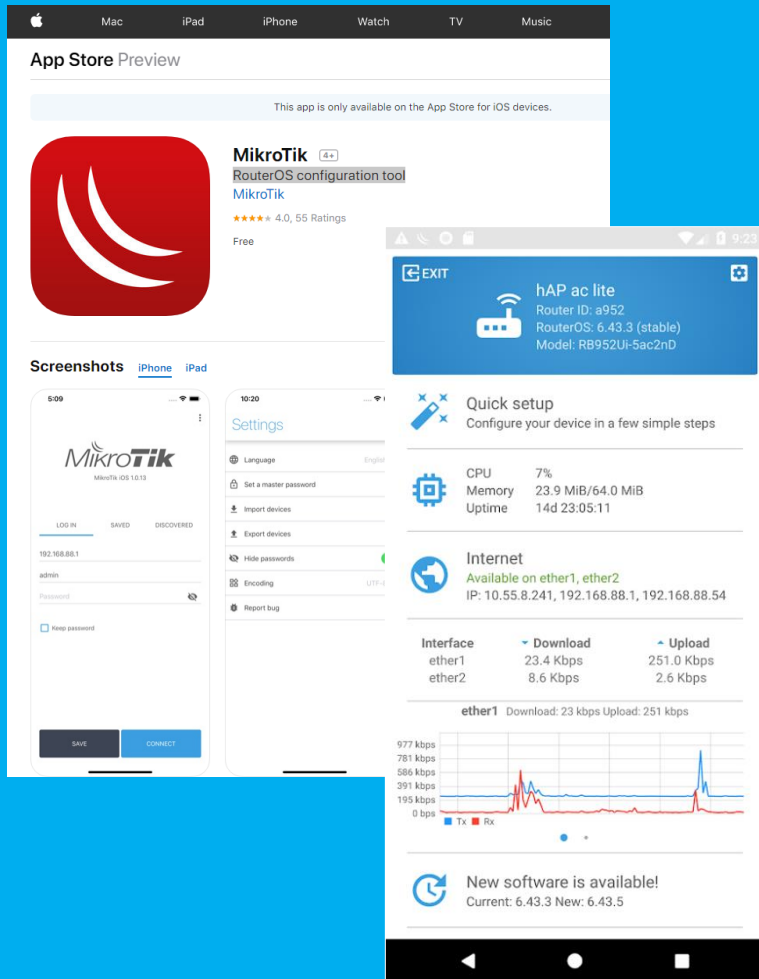
The Dude

- Сейчас как сообщу твоему начальству, что ты знал и бездействовал — тебя *транклюкируют*

- Бесплатный
- Быстро настраивается
- Визуализирует инфраструктуру
- Мониторит доступность



MikroTik (RouterOS configuration tool)



Unimus

- Резервное копирование
- Анализ (diff)
- Восстановление конфигурации

The screenshot shows the Unimus web interface with a sidebar menu on the left containing sections like Dashboard, Devices, Backups, CONFIG, IMPORT, and SETTINGS. The main content area is titled 'Mass config push' and includes a 'Name' field, a 'Status' dropdown (currently 'IDLE'), and a 'Description' field. A 'Command(s)' text area contains a script for updating the system and routerboard. Below this are checkboxes for 'Require "enable" (privileged-exec) mode' and 'Require "configure" (configuration) mode', along with a 'Select devices' button and a 'Devices: 3' count. At the bottom, there are 'Save', 'Delete', and 'Run now' buttons. A 'Last run' timestamp and an 'Output groups' table are also visible.

```
<prompt> /system package update
<prompt> set channel=stable
<prompt>
<prompt> :if ( [get status] = "System is already up to date" ) do={ /system routerboard print } else={
re) do={ /system routerboard print } } else={ print }
```

Group	Device
Output-1	1
Output-2	1

The screenshot shows the 'Backups' section of the Unimus web interface. It displays a diff view of configuration files for two different points in time. The left pane shows the configuration as of 'aug/22/2017 18:28:52 by RouterOS 6.40.1', and the right pane shows it as of 'aug/22/2017 18:42:33 by RouterOS 6.40.1'. The diff highlights changes in the configuration, such as the addition of new interfaces and the modification of existing ones. The interface includes a sidebar with navigation options like Dashboard, Devices, Backups, CONFIG, IMPORT, and SETTINGS.

- Запуск скрипта на группе устройств
- Анализ результатов с разбиением на группы
- Восстановление конфигурации (см. выше) ↑

Цветовая дифференциация штанов

Какая ожидается нагрузка по трафику (kpps, Mbps)?

Насколько сложная обработка (очереди, правила)?

Используется ли VPN

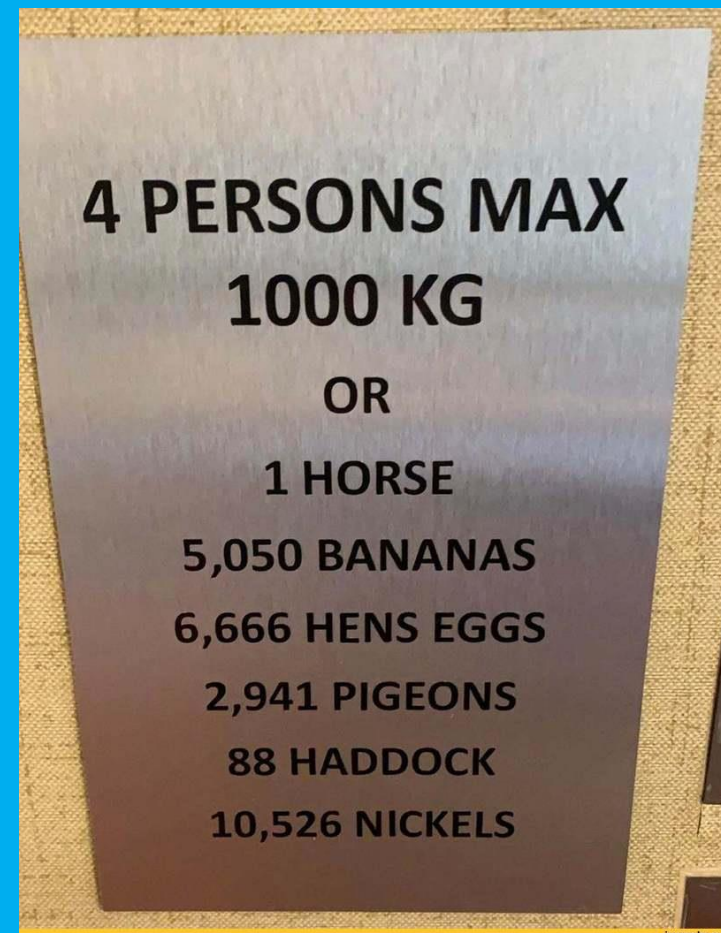
Какой еще требуется функционал (PoE, Wi-Fi, SFP)?

Общая платформа с точками доступа

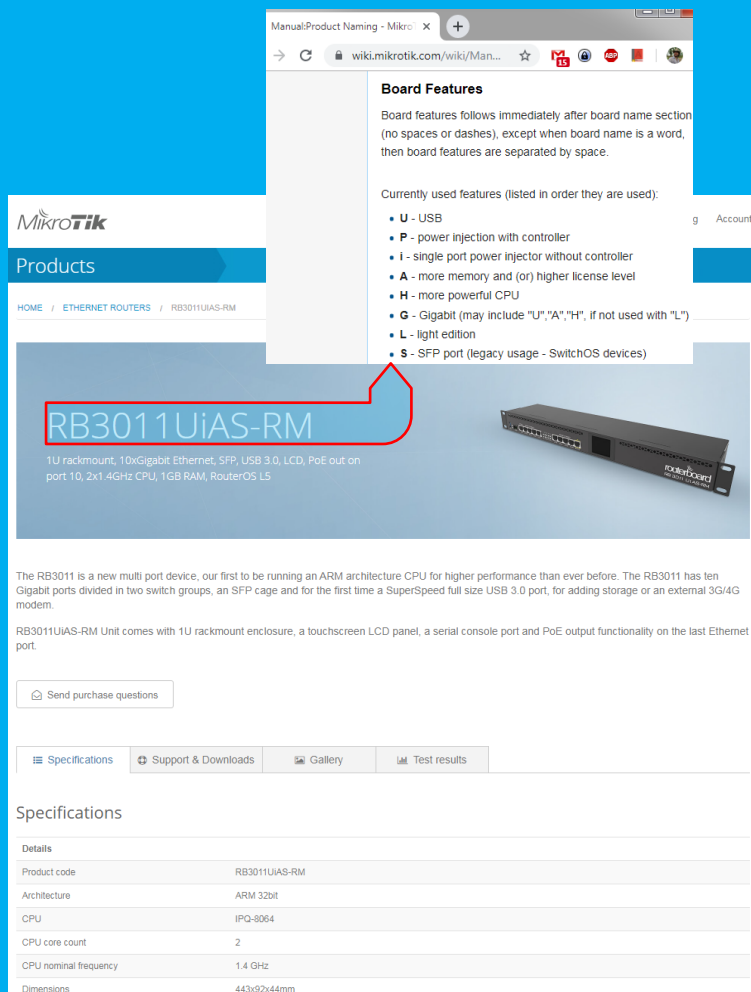
Отсутствует свитч ядра

Нужен канал через 3G-модем

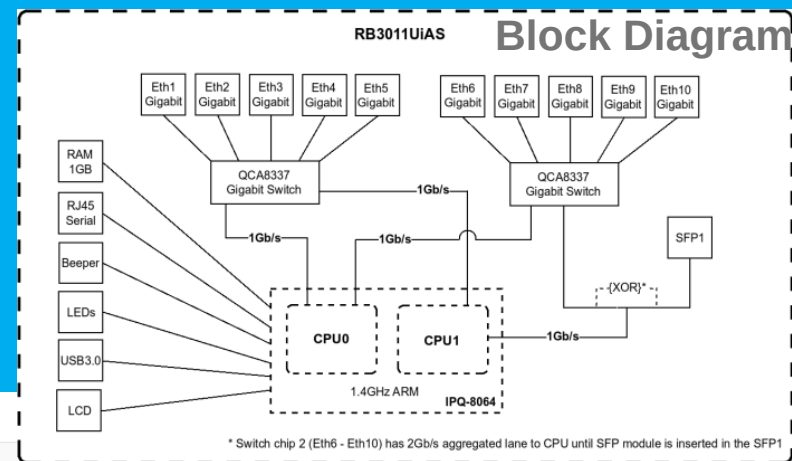
Стоечное исполнение



Выбор устройства



- Ну вот у вас, на Земле, как вы определяете — кто перед кем сколько должен присесть?
- Ну, эт на глаз...
- Дикари.



Ethernet test results

RB3011UIAS-RM		IPQ-8064 All port test					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	325.0	3,946.8	939.8	3,849.4	1,530.2	783.5
Bridging	25 bridge filter rules	325.0	3,946.8	384.2	1,573.7	348.6	178.5
Routing	none (fast path)	325.0	3,946.8	939.8	3,849.4	1,437.6	736.1
Routing	25 simple queues	325.0	3,946.8	419.6	1,718.7	419.7	214.9
Routing	25 ip filter rules	202.0	2,453.1	204.1	836.0	188.4	96.5

1. All tests are done with Xena Networks specialized test equipment (XenaBay), and done according to RFC2544 (Xena2544)
2. Max throughput is determined with 30+ second attempts with 0,1% packet loss tolerance in 64, 512, 1518 byte packet sizes
3. Test results show device maximum performance, and are reached using mentioned hardware and software configuration, different configurations most likely will result in lower results

Cloud Hosted Router

- RouterOS как виртуальная машина
- CHR + The Dude
- Минимальные требования:

Package version: RouterOS v6.34 or newer

Host CPU: 64-bit with virtualization support

RAM: 128MB or more

Disk: 128MB disk space for the CHR virtual hard drive (Max: 16GB)

Замуровали демоны!

- PowerLine устройства
- Свитч с питанием по PoE
- V-lan'ы чтобы разделить 1 провод

RouterBOARD

«One does not simply... into Mordor»

Accessories for LTE



R11e-LTE

LTE miniPCIe card for international bands.

- 2G/3G/4G/LTE miniPCIe card
- Support for international LTE bands 1/2/3/5/7/8/20/38/40
- Two U.FL connectors
- Can be used with any of MikroTik products with RouterOS and miniPCIe slot (except RB800)

mt.lv/p/341



R11e-LTE-US

LTE miniPCIe card for United States bands.

- 3G/4G/LTE miniPCIe card
- Support for US LTE bands 2/4/5/12
- Two U.FL connectors
- Can be used with any of MikroTik products with RouterOS and miniPCIe slot (except RB800)

mt.lv/p/342



R11e-4G

Category 4 4G/LTE miniPCI-e card.

- R11e-4G supports LTE FDD bands 3 (1800MHz), 7 (2600MHz), 20 (800MHz) and 31 (450MHz), as well as LTE TDD bands 41n (2500MHz), 42 (3500MHz) and 43 (3700MHz).
- Compatible with our products that has miniPCIe slots, like LtAP mini, wAP R, RBM11G, RBM33G or others

mt.lv/p/433



AC SMAUFL

U.FL-SMA female pigtail.

- To be used to connect an LTE card to an external antenna
- U.FL connector on one side, SMA female on other
- Designed for use with the wAP R

mt.lv/p/337



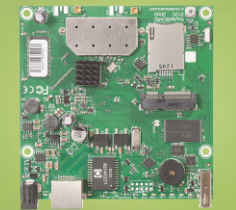
[Home](#) [About](#) [Buy](#) [Jobs](#) [Hardware](#) [Software](#) [Support](#) [Training](#) [Account](#)

Products

[HOME](#) / [ROUTERBOARD](#) / [RB912UAG-2HPnD](#)

RB912UAG-2HPnD

600MHz CPU, 64MB RAM, 1xGigabit Ethernet, onboard 2.4Ghz wireless, miniPCI-express, USB, SIM slot, RouterOS L4



The RB912UAG-2HPnD is a very versatile device. It is a small wireless router with an integrated 2.4GHz high power wireless card and an additional miniPCI slot for 802.11 wireless, or 3G card. The Gigabit port helps to utilize the full potential of 802.11n wireless speeds.

It has built in 16kV ESD protection on both the Ethernet and the MMCX ports.

Send purchase questions

Specifications

Support & Downloads

Gallery

Test results

Specifications

Details

Product code	RB912UAG-2HPnD
CPU	AR9342

Заключение



A fluffy grey kitten is the central focus, sitting on a white surface. It has large, round, light-colored eyes and is looking directly at the camera. In the background, a beige sofa is visible against a light-colored wall. The entire image is framed by a bright blue border.

КОТЕ

*Мікро***Tik**

одобряет