

Программные средства анализа беспроводных сетей радиодоступа

Практики 1

Специализированные утилиты мониторинга

- Утилита **nslookup** предназначена для формирования запросов к серверам DNS из командной строки. Она является аналогом службы DNS-клиент и позволяет диагностировать проблемы с разрешением имен в системе DNS. По умолчанию все запросы отправляются на DNS-сервер, адрес которого задан настройками сетевого подключения. В терминах утилиты такой сервер является сервером по умолчанию (default server). Утилита nslookup позволяет определить как адреса IPv4, так и IPv6.
- Утилита **ping** формирует эхо-запросы и эхо-ответы с использованием пакетов протокола ICMP. Принцип работы утилиты подразумевает получение ответа только от конечного узла.
- Утилита **tracert** (tceroute для решений на Linux) обычно используется совместно с утилитой ping и позволяет уточнить проблемы на сети. Для формирования запросов и ответов также используется протокол ICMP, но для определения доступности промежуточных узлов используется манипулирование значением TTL.

```

Выбрать Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Админ>nslookup mail.yandex.ru
DNS request timed out.
    timeout was 2 seconds.
<x>EtxE: Unknown
Address: fe80::261f:a0ff:fe0d:3373

DNS request timed out.
    timeout was 2 seconds.
*** Превыshено время ожидания запроса Unknown

C:\Users\Админ>ping yandex.kz

Обмен пакетами с yandex.kz [5.255.255.5] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 5.255.255.5: число байт=32 время=85мс TTL=52      работа утилиты
Ответ от 5.255.255.5: число байт=32 время=98мс TTL=52      ping: первый
Ответ от 5.255.255.5: число байт=32 время=80мс TTL=52      эхо-запрос потерян

Статистика Ping для 5.255.255.5:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    <25% потеря>
Приблизительное время приема-передачи в мс:
    Минимальное = 80мсек, Максимальное = 98 мсек, Среднее = 87 мсек

C:\Users\Админ>tracert yandex.kz

Трассировка маршрута к yandex.kz [5.255.255.5]      работа утилиты tracert
с максимальным числом прыжков 30:

  1      3 ms      2 ms      1 ms  192.168.0.1
  2      *          *          *      Превышен интервал ожидания для запроса.
  3    821 ms     21 ms     24 ms  10.9.0.221
  4    29 ms      19 ms     20 ms  10.9.8.137
  5    24 ms      17 ms     18 ms  84.240.234.4
  6    84 ms      61 ms     61 ms  95.59.172.14
  7    46 ms      57 ms     39 ms  95.59.172.13
  8    51 ms      59 ms     40 ms  95.59.172.19
  9    73 ms      73 ms     75 ms  yandex-2-ix.giganet.ua [91.245.221.101]
 10   102 ms     81 ms     77 ms  neun-xe-3-0-3.yndx.net [213.180.213.6]
 11    90 ms      74 ms     80 ms  m9-p1-be1.yndx.net [87.250.239.22]
 12    93 ms      75 ms     72 ms  ugr-b-c1-ae5.yndx.net [87.250.239.53]
 13    77 ms      76 ms     *      yandex.ru [5.255.255.5]
 14    79 ms      78 ms     77 ms  yandex.ru [5.255.255.5]

Трассировка завершена.

```

работа утилиты
nslookup: DNS-
сервер не отвечает

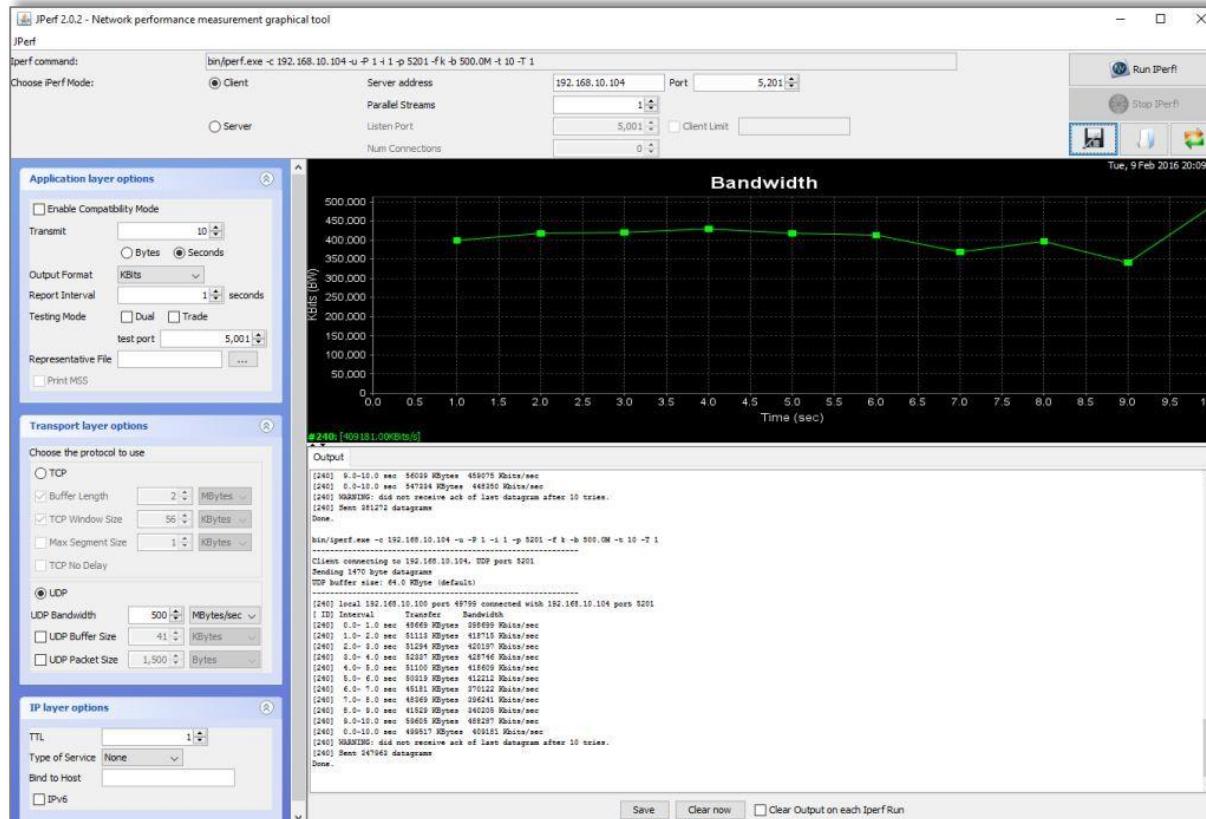
работа утилиты
ping: первый
эхо-запрос потерян

работа утилиты tracert

Утилиты используют IP-сеть, поэтому применяются только в случае реализации сетевой среды TCP/IP. Не подходят для анализа физических свойств радиоканала, но отражают доступность сетевой среды. Могут применяться для сетей любых размеров, от PAN до WAN.

Утилита iperf

- Утилита iperf не является стандартной утилитой, но часто используется в качестве средства оценки пропускной способности соединения. Представляет собой генератор трафика TCP и UDP, имеет широкий спектр опций, позволяющих проводить гибкую политику оценки пропускной способности.



Утилита также имеет графическую оболочку jperf, облегчающую управление опциями генератора трафика и визуализирующую результаты измерений.

```
C:\iperf>iperf3 -s
-----  
серверный режим  
Server listening on 5201  номер прослушиваемого порта  
-----  
Accepted connection from 192.168.10.100, port 59488  
[ 5] local 192.168.10.104 port 5201 connected to 192.168.10.100 port 59489  
[ ID] Interval      Transfer     Bandwidth  
[ 5]  0.00-1.01  sec   228 KBytes  1.86 Mbits/sec  
[ 5]  1.01-2.01  sec   206 KBytes  1.69 Mbits/sec  
[ 5]  2.01-3.01  sec   606 KBytes  4.93 Mbits/sec  
[ 5]  3.01-4.00  sec   550 KBytes  4.56 Mbits/sec  
[ 5]  4.00-5.00  sec   1.63 MBytes 13.7 Mbits/sec  
[ 5]  5.00-6.00  sec   1.64 MBytes 13.8 Mbits/sec  
[ 5]  6.00-7.00  sec   1.72 MBytes 14.5 Mbits/sec  
[ 5]  7.00-8.00  sec   1.61 MBytes 13.5 Mbits/sec  
[ 5]  8.00-9.00  sec   1.36 MBytes 11.4 Mbits/sec  
[ 5]  9.00-10.00 sec   38.5 KBytes  315 Kbits/sec  
[ 5] 10.00-10.06 sec   0.00 Bytes   0.00 bits/sec  
-----  
[ ID] Interval      Transfer     Bandwidth  
[ 5]  0.00-10.06 sec   0.00 Bytes   0.00 bits/sec  
[ 5]  0.00-10.06 sec   9.56 MBytes  7.97 Mbits/sec  
-----  
sender  
receiver  
-----  
Server listening on 5201  
-----  
iperf3: interrupt - the server has terminated
```

Пример работы утилиты
iperf3 в серверном режиме

```
C:\iperf3>iperf3 -c 192.168.10.104
Connecting to host 192.168.10.104, port 5201
[ 4] local 192.168.10.100 port 59489 connected to 192.168.10.104 port 5201
[ ID] Interval      Transfer     Bandwidth  
[ 4]  0.00-1.00  sec   384 KBytes  3.15 Mbits/sec  
[ 4]  1.00-2.00  sec   256 KBytes  2.10 Mbits/sec  
[ 4]  2.00-3.00  sec   512 KBytes  4.19 Mbits/sec  
[ 4]  3.00-4.00  sec   640 KBytes  5.24 Mbits/sec  
[ 4]  4.00-5.00  sec   1.62 MBytes 13.6 Mbits/sec  
[ 4]  5.00-6.00  sec   1.75 MBytes 14.7 Mbits/sec  
[ 4]  6.00-7.00  sec   1.62 MBytes 13.6 Mbits/sec  
[ 4]  7.00-8.00  sec   1.62 MBytes 13.6 Mbits/sec  
[ 4]  8.00-9.00  sec   1.38 MBytes 11.5 Mbits/sec  
[ 4]  9.00-10.00 sec   0.00 Bytes   0.00 bits/sec  
-----  
[ ID] Interval      Transfer     Bandwidth  
[ 4]  0.00-10.00 sec   9.75 MBytes  8.18 Mbits/sec  
[ 4]  0.00-10.00 sec   9.56 MBytes  8.02 Mbits/sec  
-----  
sender  
receiver  
-----  
iperf Done.
```

Пример работы iperf3 в
клиентском режиме

WireShark

Нужный инструмент! Необходимо
поставить себе на комп для выполнения
лаб и практик. Он бесплатный по
умолчанию, но есть платные расширения.



Анализатор трафика, реализуется для ОС Windows (не предоставляет возможность просмотра канального уровня со служебной информацией) и Linux (содержит инструменты для анализа сетей IEEE).

Возможности:

- Анализ структуры пакета вплоть уровня MAC
- Анализ статистических свойств трафика: размеров пакетов, времени прихода пакетов, интенсивности трафика, протоколов и т.п.
- Генератор трафика
- Анализ контента
- Отдельный инструмент для работы с телефонией
- Отдельный инструмент для работы с беспроводными сетями

Capturing from Беспроводная сеть

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination
537	157.633110	192.168.10.105	217.69.139.
538	157.633621	192.168.10.105	217.69.139.
539	157.645768	217.69.139.58	192.168.10.105
540	157.650489	217.69.139.58	192.168.10.105
541	157.651148	217.69.139.58	192.168.10.105
542	157.651191	192.168.10.105	217.69.139.58
543	158.846069	192.168.10.1	224.0.0.1
544	159.023306	192.168.10.105	224.0.0.251
545	159.023485	192.168.10.105	224.0.0.252
546	159.023587	192.168.10.105	239.255.255.250
547	163.106388	HuaweiTe_b1:78:95	Broadcast
548	163.856421	fe80::ea5a:a7ff:fe0... ff02::1	ICMPv6
549	164.505003	192.168.10.105	5.255.255.5
550	164.518141	5.255.255.5	192.168.10.105
551	167.660458	192.168.10.105	217.69.139.58
552	167.673095	217.69.139.58	192.168.10.105

Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0

Ethernet II, Src: IntelCor_6d:1e:29 (9c:da:3e:6d:1e:29), Dst: LlcEmzio_00:0e:f7 (e8:5a:a7:00:0e:f7)

- > Destination: LlcEmzio_00:0e:f7 (e8:5a:a7:00:0e:f7)
- > Source: IntelCor_6d:1e:29 (9c:da:3e:6d:1e:29)
- Type: IPv4 (0x0800)

Internet Protocol Version 4 Src. 192.168.10.105 Dst. 52.86.19.108

0000	e8 5a a7 00 0e f7 9c da 3e 6d 1e 29 08 00 45 00	.Z.....>m.)..E.
0010	00 29 5a fa 40 00 80 06 8c a7 c0 a8 0a 69 34 56	.)Z@.....i4V
0020	13 c6 c8 e4 01 bb 53 bd 0d 23 05 99 ba 80 50 10S. #....P.
0030	01 04 b0 08 00 00 00

Беспроводная сеть: <live capture in progress>

Packets: 552 · Displayed: 552 (100.0%)

Profile: Default

CommView for WiFi

Анализатор трафика для Wi-Fi сетей.
Платный, но имеет оценочную
версию с ограниченным
функционалом

CommView for WiFi - Оценочная версия

Файл Поиск Вид Инструменты Настройка Правила Справка

Узлы Каналы Текущие IP-соединения Пакеты VoIP Log-файлы Правила Предупреждения

Использование, 2,4 GHz, МБ/сек

Использование, 5,0 GHz, МБ/сек

Уровень сигнала, 2,4 GHz, dBm

Уровень сигнала, 5,0 GHz, dBm

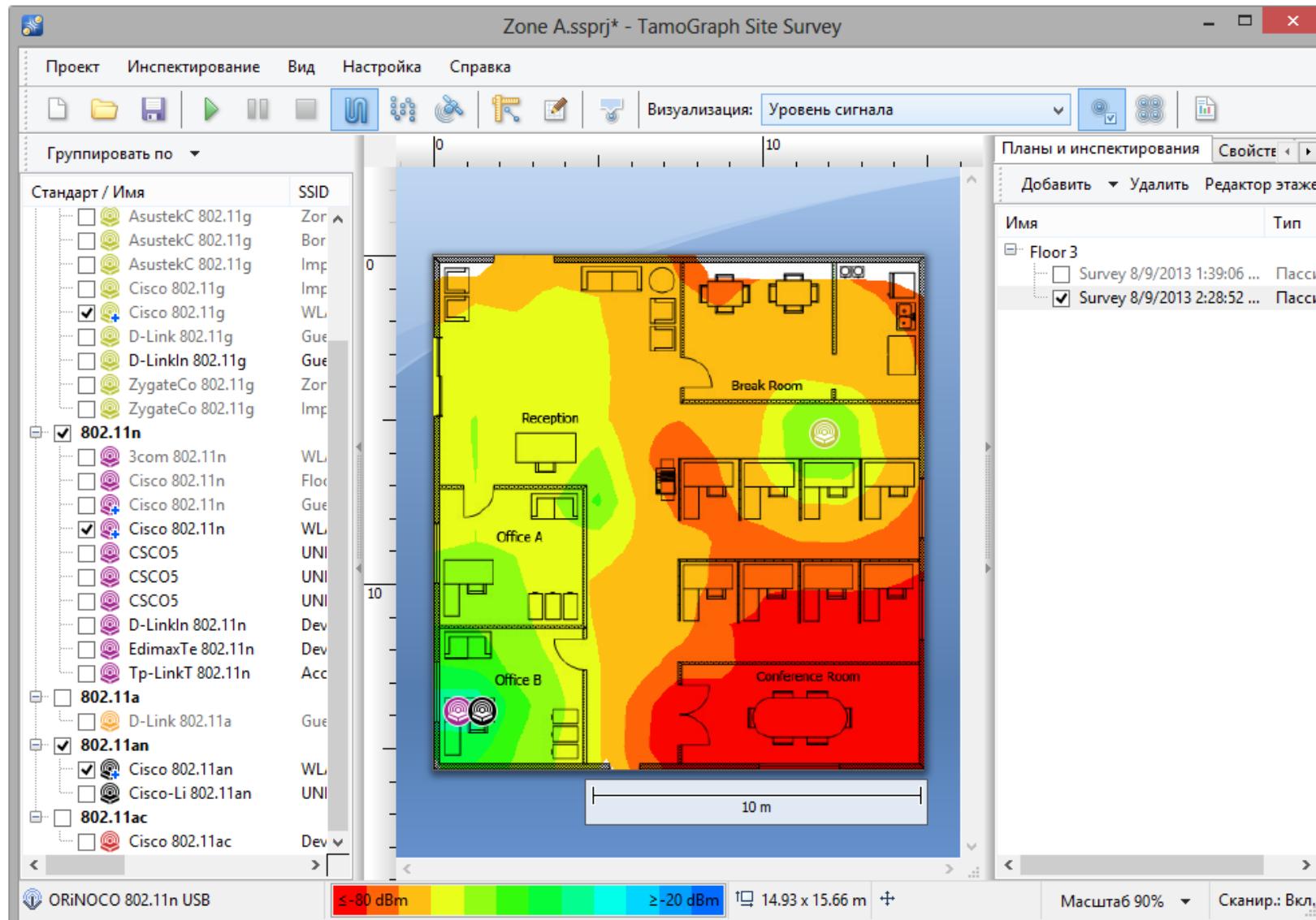
Стандарт / МА... Канал Тип SSID Стандарт Шифрование Сигнал Макс. ск... Пото... Скорость (Tx) Скорость (Rx) Байты

802.11n

SSID	Сигнал	Макс. ск...	Пото...	Скорость (Tx)	Скорость (Rx)	Байты
Tp-Link...	-78/-63/-60	150,0	1	1/1/1	0/0/0	
Cisco:E9...	-77/-72/-69	144,0	2	1/1/1	0/0/0	
Cisco:E9...	-76/-72/-69	144,0	2	1/1/1	0/0/0	
Cisco:4B...	-74/-72/-65	144,0	2	1/1/1	0/0/0	
Cisco:4B...	-62/-59/-57	144,0	2	1/1/1	0/0/0	
Cisco:4B...	-73/-59/-57	144,0	2	1/1/1	0/0/0	
Cisco:4B...	-76/-59/-57	144,0	2	1/1/1	0/0/0	
Cisco:4B...	-72/-59/-57	144,0	2	1/1/1	0/0/0	
Cisco:4B...	-62/-59/-57	144,0	2	1/1/1	0/0/0	
Cisco:0F...	-75/-72/-66	144,0	2	1/1/1	0/0/0	
Cisco:0F...	-76/-72/-69	144,0	2	1/1/1	0/0/0	
Cisco:0F...	-76/-71/-68	144,0	2	1/1/1	0/0/0	
Cisco:0F...	-72/-66/-61	144,0	2	1/1/1	0/0/0	
Cisco:0F...	-71/-66/-61	144,0	2	1/1/1	0/0/0	
Cisco:0F...	-71/-66/-61	144,0	2	1/1/1	0/0/0	
SSID	Сигнал	Макс. ск...	Пото...	Скорость (Tx)	Скорость (Rx)	Байты
Cisco:49...	-86/-64/-61	144,0	2	6/6/6	0/0/0	
Cisco:49...	-86/-64/-61	144,0	2	6/6/6	0/0/0	
Cisco:49...	-85/-65/-61	144,0	2	6/6/6	0/0/0	
Cisco:49...	-85/-64/-61	144,0	2	6/6/6	0/0/0	
Cisco:49...	-85/-64/-61	144,0	2	6/6/6	0/0/0	
Cisco:0F...	-76/-74/-66	144,0	2	6/6/6	0/0/0	
Cisco:0F...	-76/-73/-66	144,0	2	6/6/6	0/0/0	
Cisco:0F...	-78/-74/-64	144,0	2	1/6/6	0/0/0	

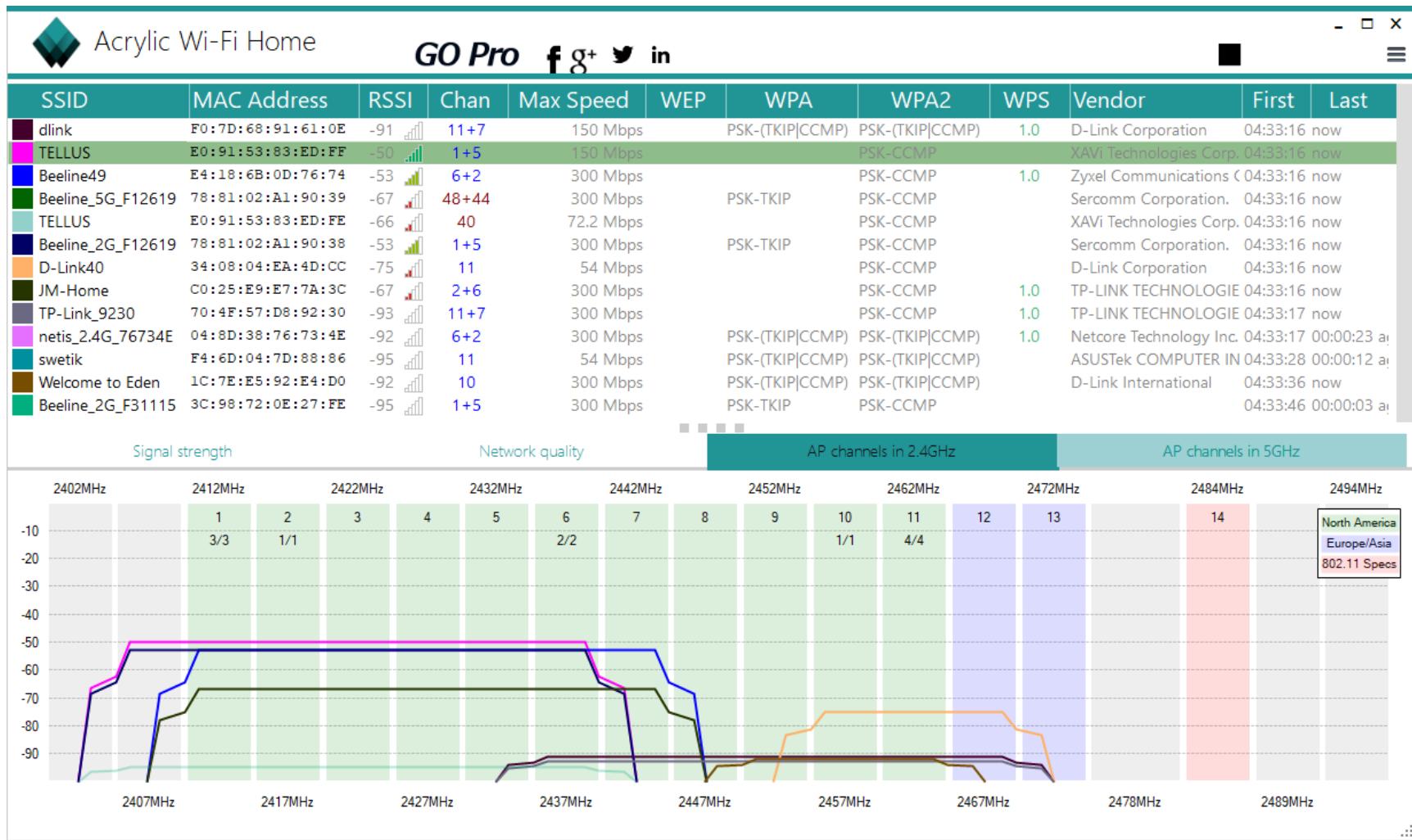
TamoGraph® Site Survey

ПО для инспектирования Wi-Fi сетей.
Платный, но имеет оценочную
версию с ограниченным
функционалом



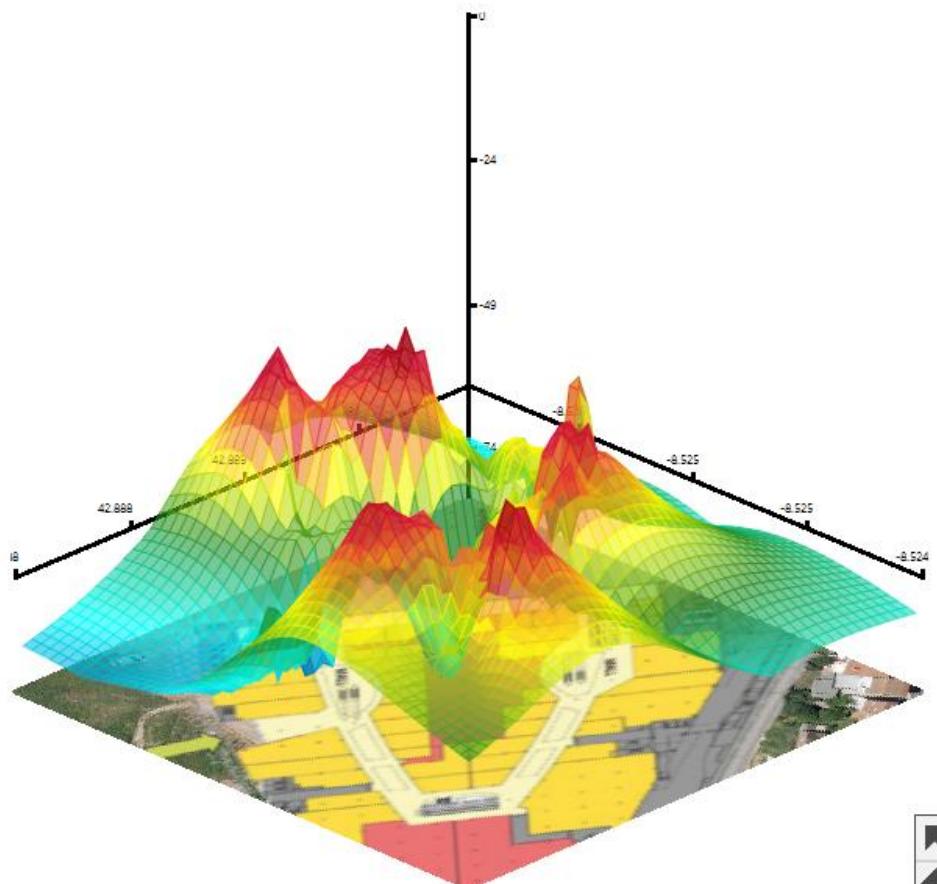
Acrylic Wi-Fi

Семейство ПО для анализа Wi-Fi сетей
www.acrylicwifi.com

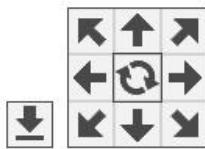




Acrylic Wi-Fi HeatMaps



3D



Working Location: 0 - Main floor - Supermarket and Mall

Plots

Access Points

Routes



Layers

Select

Network	#	2.4	5
Lois	1	1	
Pans&Company	1	1	
AsCancelas	25	23	
Carrefour-Conecta	10	6	4
O CODICE	1	1	
SMOOY WIFI	1	1	
IMAGINARIUM	1	1	
Internacional	1	1	
Tenda R	1	1	
Lois 2	1	1	
Brasylone	1	1	



Min RSSI (dBm): -99

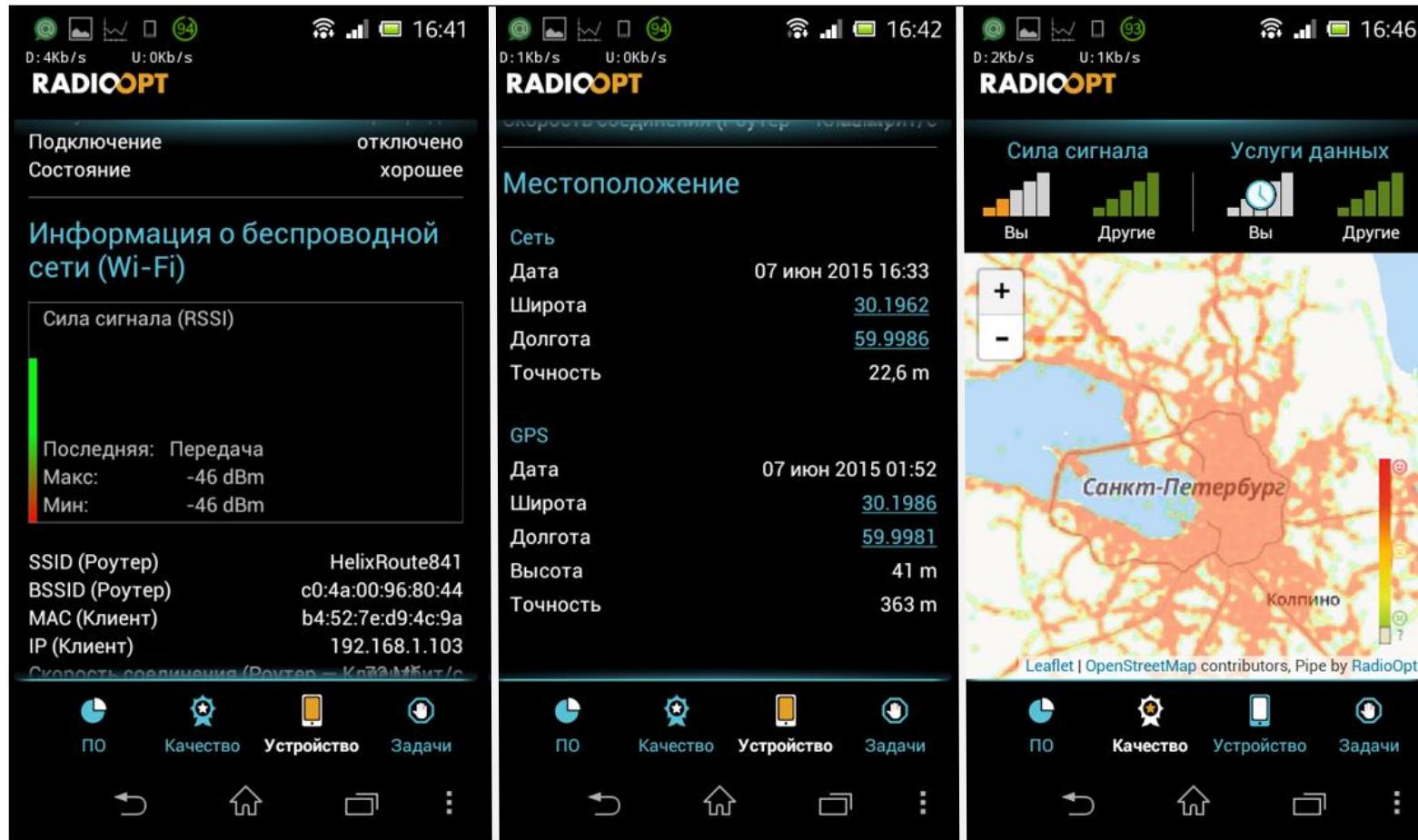
Opacity: 75%

Z Axis at level -64

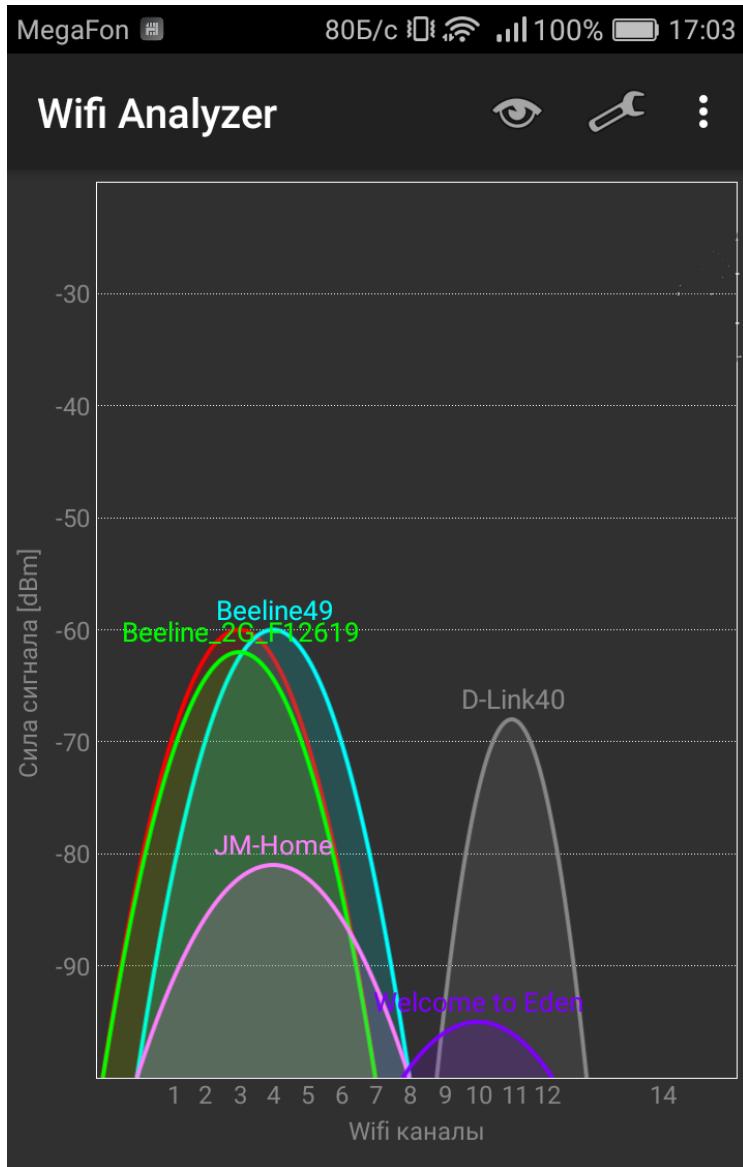
Rssi Scale: 50%

Примеры приложений для телефонов

- Traffic Monitor



Для анализа сетей Wi-Fi



Для анализа сетей мобильной связи

