



**ВМК МГУ**

Факультет вычислительной математики и кибернетики  
Московского государственного университета имени М. В. Ломоносова

## **Программно определяемое радио - SDR. Протокол CAPWAP.**

Москва, 21 апреля 2016

***Сергей Монин***

# План:

1. Программно определяемое радио – SDR
  - 1.1 Предпосылки
  - 1.2 Современные решения
  - 1.3 ПО
2. Протокол CAPWAP
  - 2.1 История появления и развития
  - 2.2 Принципы работы
  - 2.3 Безопасность
  - 2.4 Интеграция с ПКС сетями

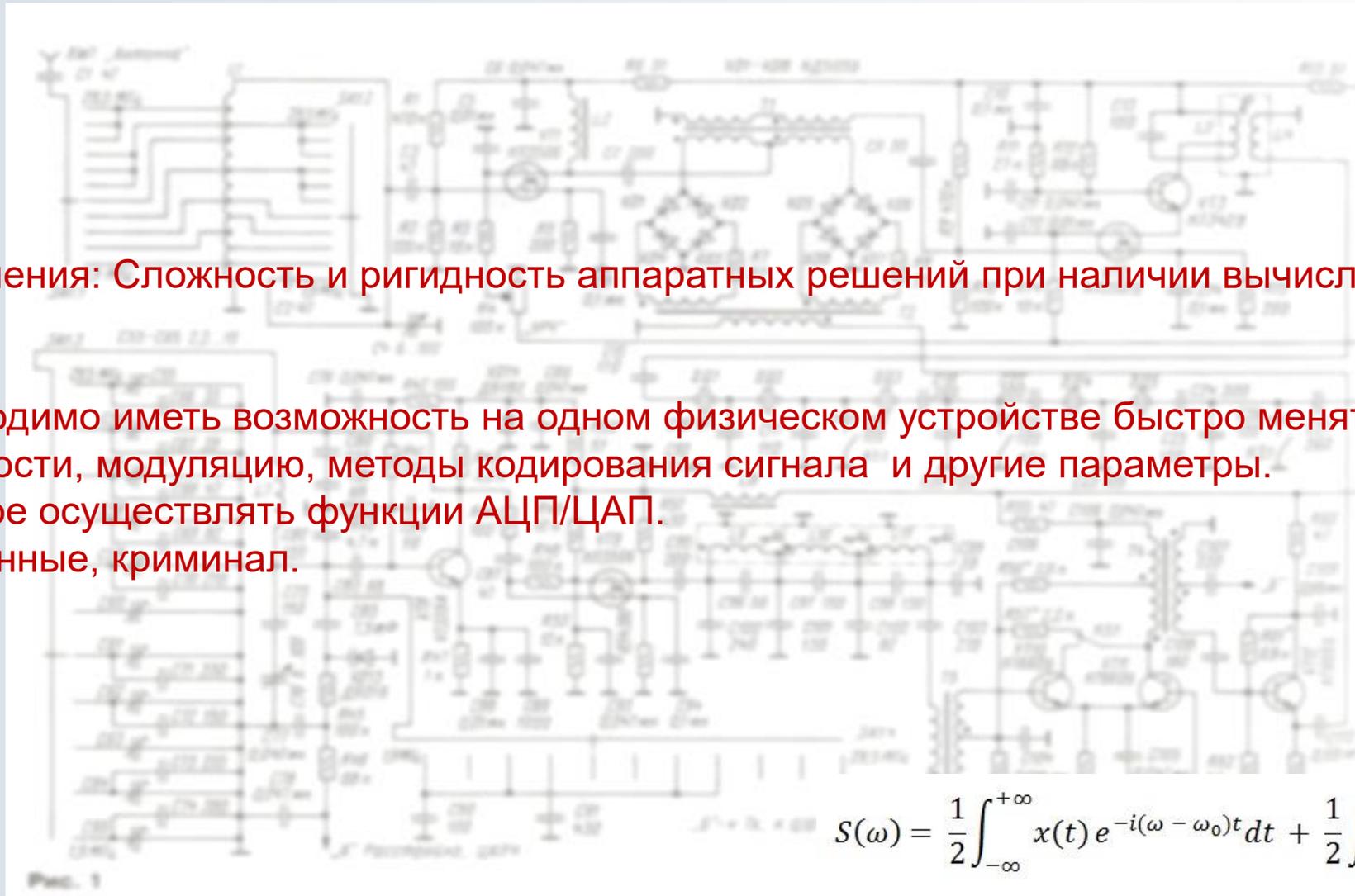
# Программно определяемое радио – SDR

Причины появления: Сложность и ригидность аппаратных решений при наличии вычислительных ресурсов

Задача: Необходимо иметь возможность на одном физическом устройстве быстро менять рабочие частоты, мощности, модуляцию, методы кодирования сигнала и другие параметры.

И самое главное осуществлять функции АЦП/ЦАП.

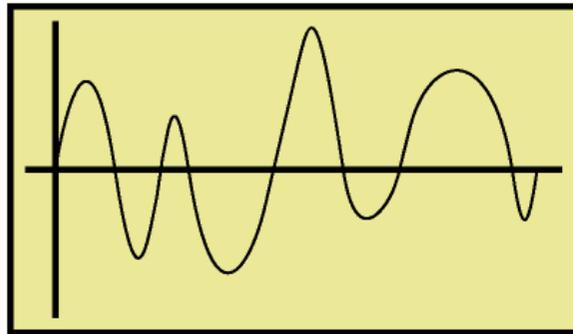
Заказчики: Военные, криминал.



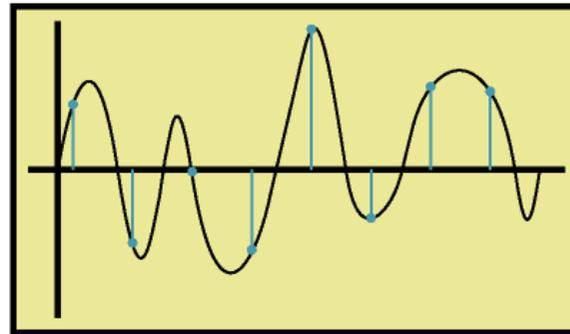
$$S(\omega) = \frac{1}{2} \int_{-\infty}^{+\infty} x(t) e^{-i(\omega - \omega_0)t} dt + \frac{1}{2} \int_{-\infty}^{+\infty} x(t) e^{-i(\omega + \omega_0)t} dt$$

# Программно определяемое радио – CDR

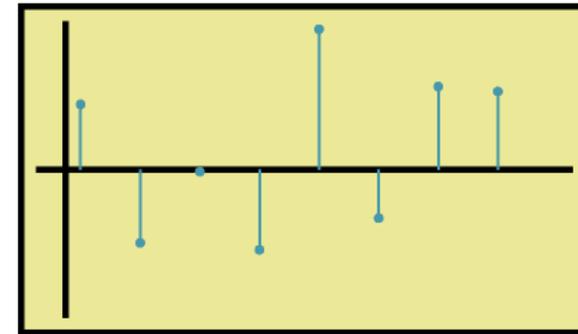
Аналоговый сигнал необходим потребителю (ухо/рот). В других местах удобнее иметь дело с цифровым сигналом => требуется преобразование аналогового сигнала в цифровой и обратно.



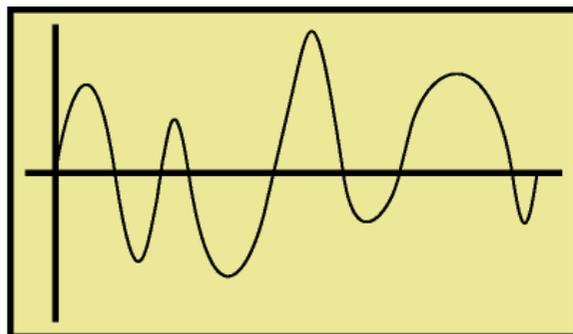
**Analog Audio Source**



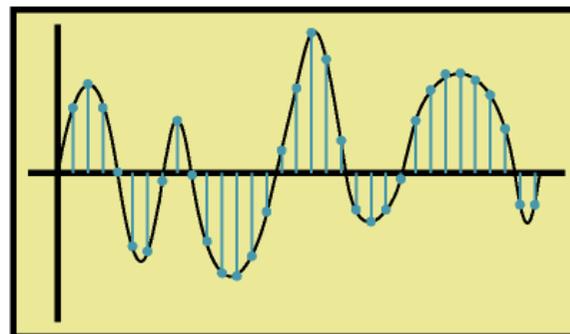
**Low Sampling Rate**



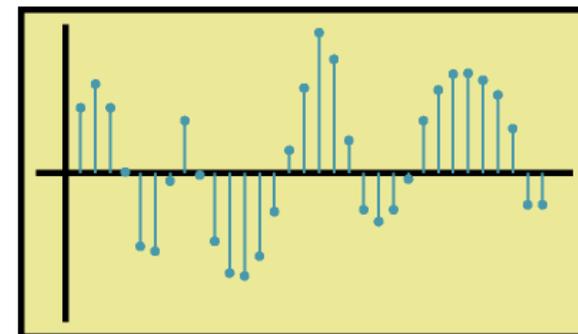
**High Information Loss**



**Analog Audio Source**



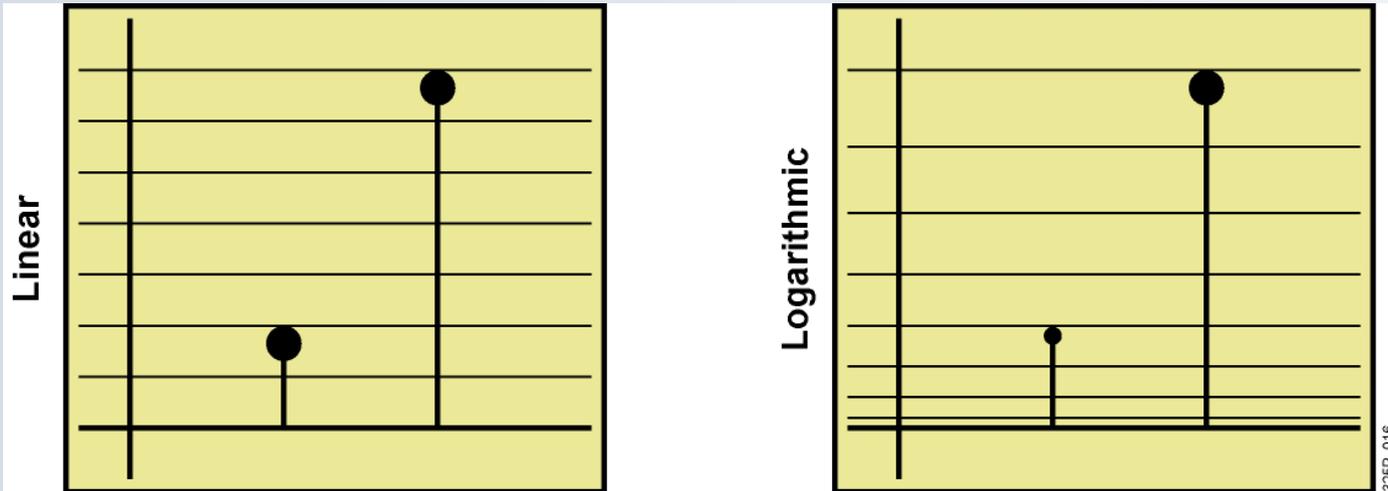
**High Sampling Rate**



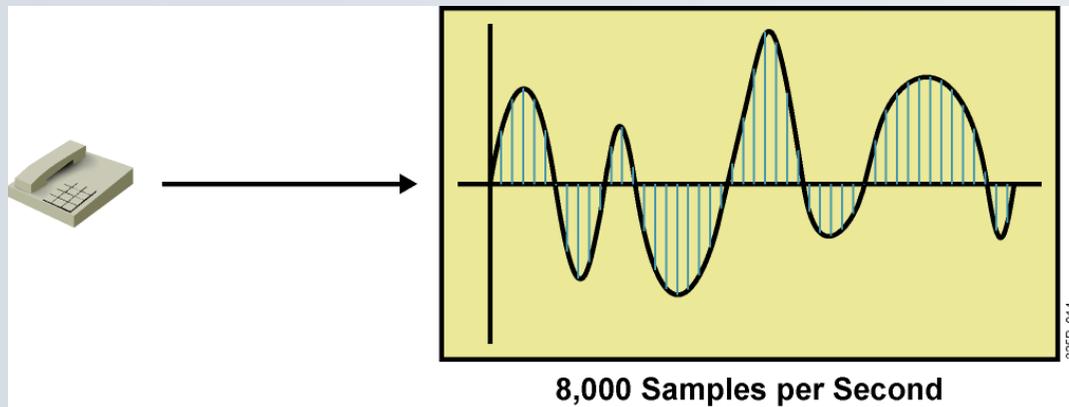
**Low Information Loss**

# Программно определяемое радио – SDR

## Техники квантизации



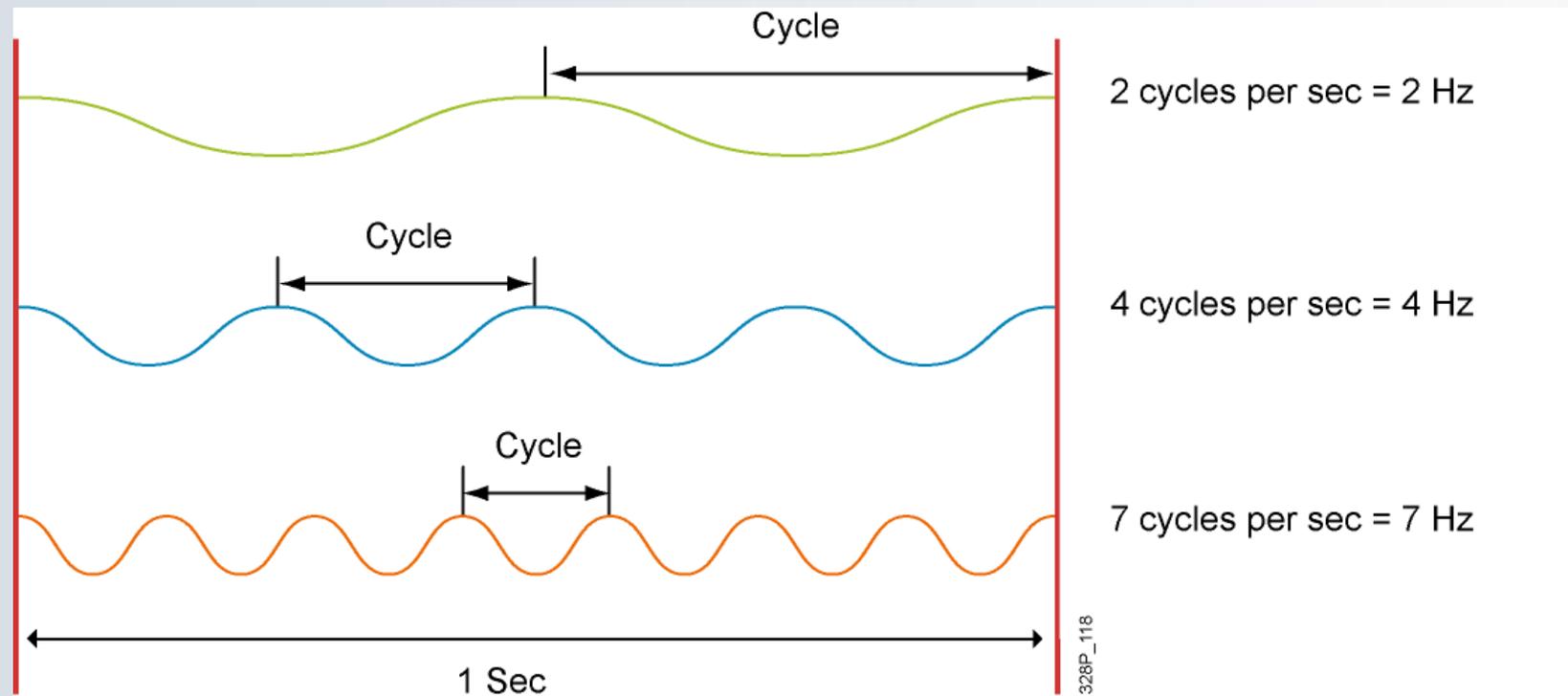
## Полосы пропускания



Standard, Codec	Bit Rate (kbps)	Voice Quality (MOS)
G.711	64	4.1
G.726	16, 24, 32	3.85 (with 32 kbps)
G.728	16	3.61
G.729	8	3.92

# Программно определяемое радио – SDR

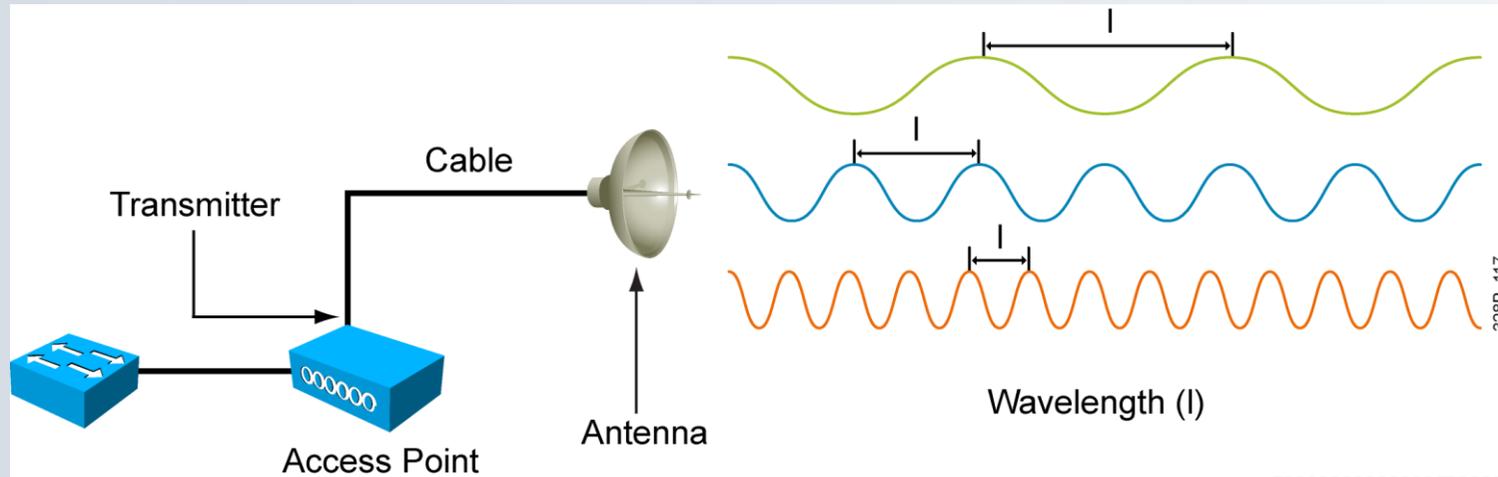
При передаче сигнала в эфир его нужно про-модулировать (AM, FM, PHASE-M)



Частота

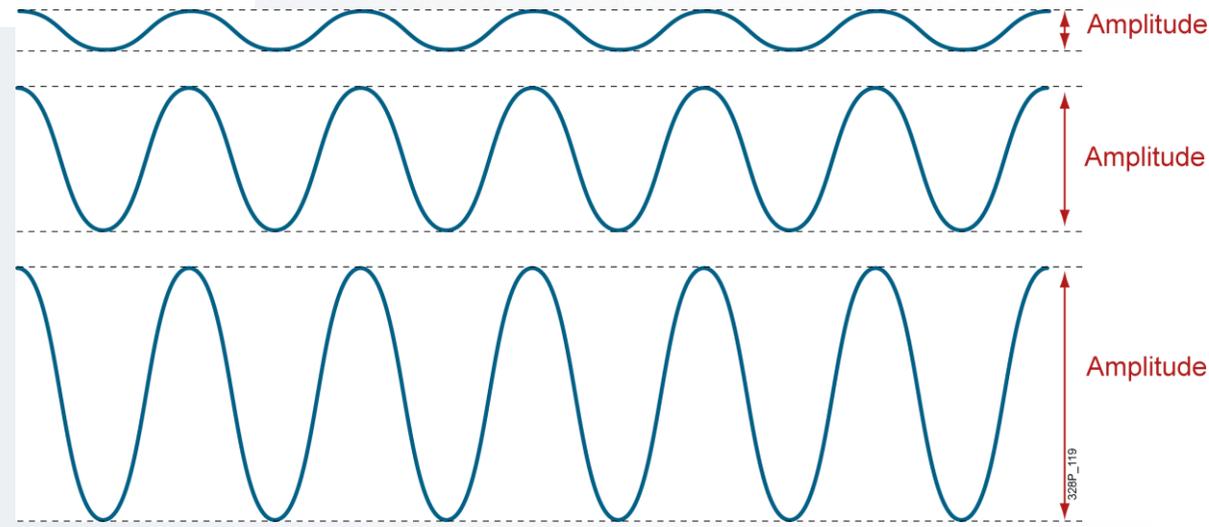
# Программно определяемое радио – SDR

При передаче сигнала в эфир его нужно про-модулировать (AM, FM, PHASE-M)



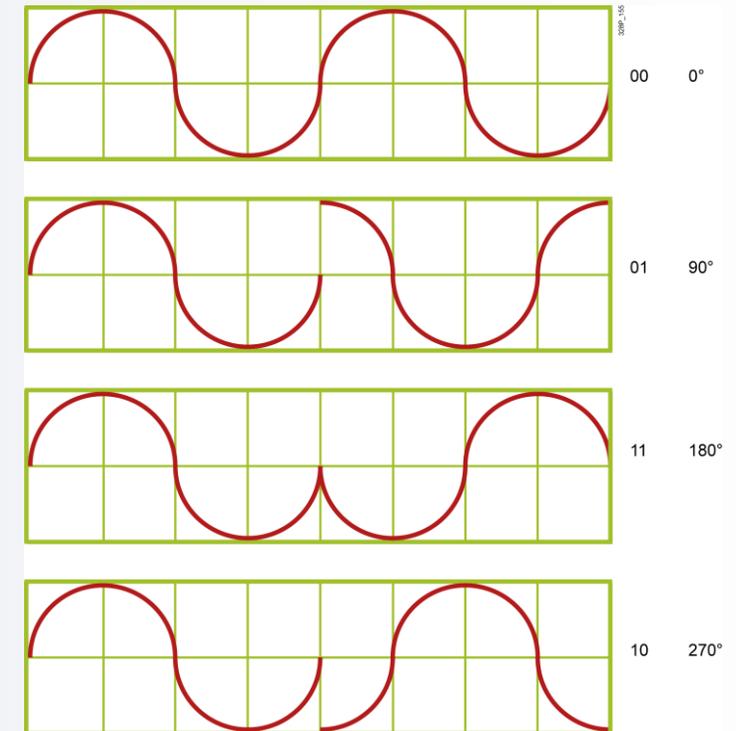
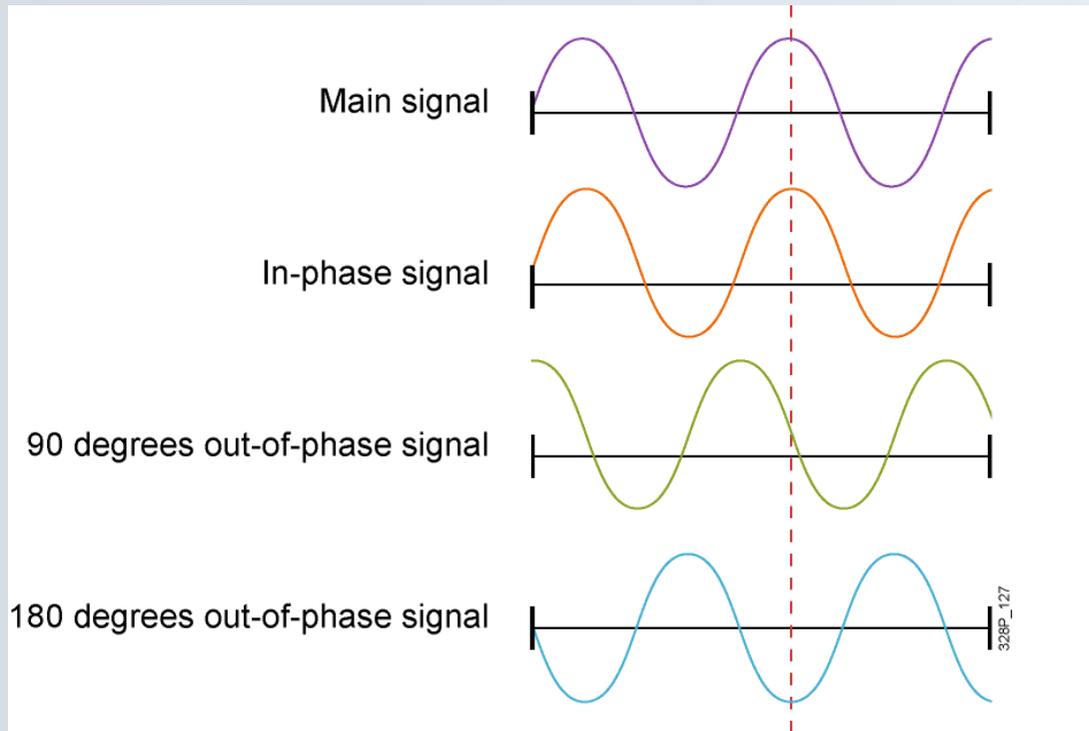
Длина волны

Амплитуда



# Программно определяемое радио – SDR

При передаче сигнала в эфир его нужно про-модулировать (AM, FM, PHASE-M)



Пример фазовой модуляции QPSK  
4 фазы – 2 бита за квант

# Программно определяемое радио – SDR

Практическая польза:

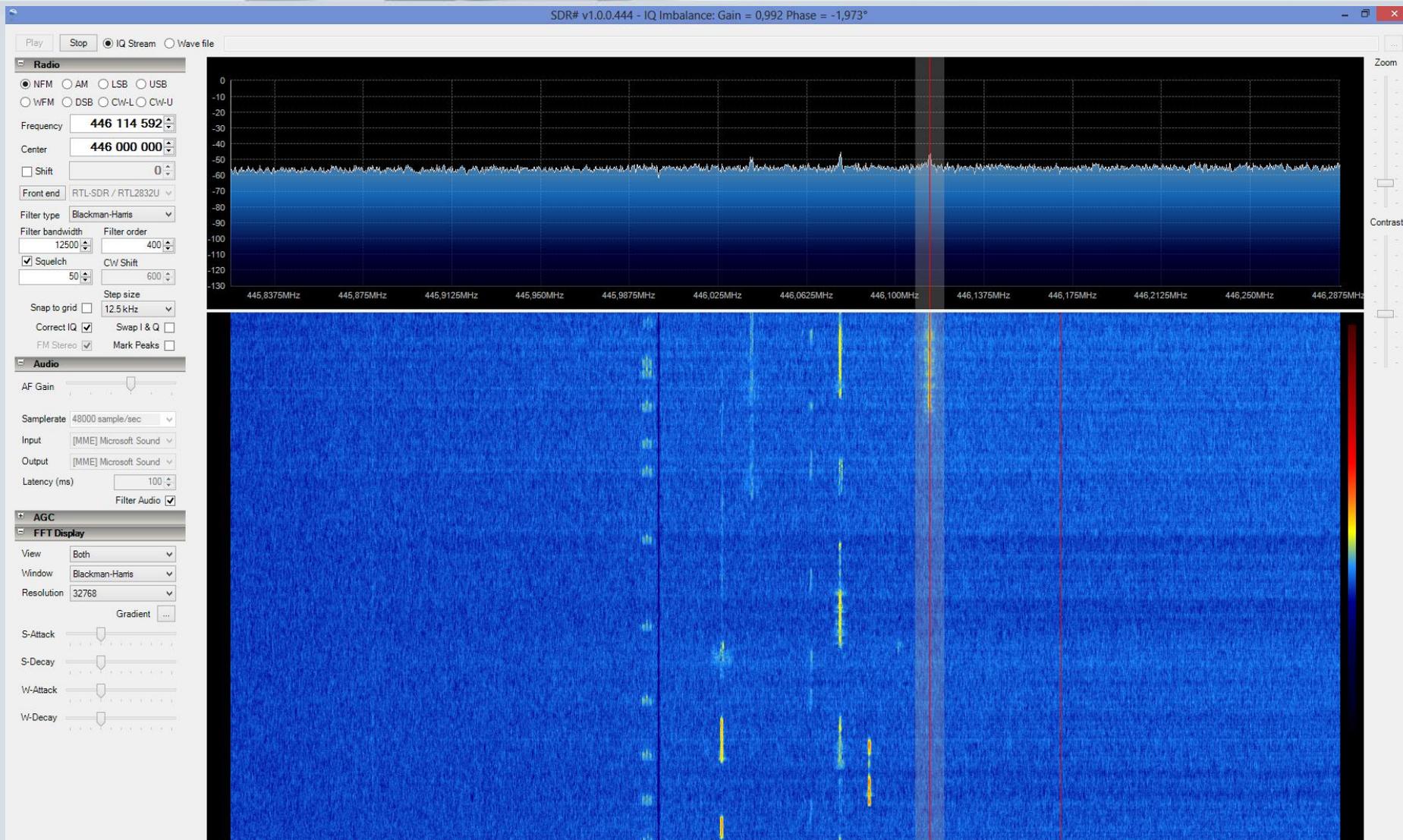
- в промышленности построение радиосистем упростилось в сотни раз
- почти любая вычислительная система готова решать задачи обработки радиосигнала, нужно только завести его внутрь!



RTL2832 и E4000 в сумме от 24 до 2200МГц  
RtlSDR.dll , SDRSharp, антенна. Это все что нужно для начала.

Для продолжения – ПО мощный конструктор GNU Radio, расширители диапазонов, малошумный усилитель

# Программно определяемое радио – SDR



Выбери метод демодуляции (Авиа-AM, Радио-FM, NFM), диапазон частот. Плагин Autotuner может найти все каналы, где идет передача сигнала.

Полиция P25 (ПО декодер DSD)  
Рации 27 МГц (антенна 2.39м)  
Авиа переговоры 117-135МГц AM  
Авиа ADS-B 1090МГц (ПО декодер)  
КВ 8-15МГц (Ночь)

Отладка радиопередатчиков,  
Анализ DECT,  
аналоговых радиотелефонов,  
Для разбора протоколов связи в  
радиоуправлении, пультов,  
погодных станций, систем удаленного  
сбора информации с датчиков,  
счетчиков. GSM/MeteoСпутники/GPS...

**You have been warned !  
...twice.**

# Программно определяемое радио – SDR пример сервиса:

**DP156 /PBD156**  
POBEDA

**FLIGHT STATUS**

**KRR** KRASNODAR **VKO** MOSCOW

SCHEDULED DEPARTURE	13:15	SCHEDULED ARRIVAL	15:35
ACTUAL DEPARTURE	13:29	ESTIMATED ARRIVAL	15:15
AVERAGE FLIGHT TIME	02:09	AVERAGE DELAY	00:57

GREAT CIRCLE DISTANCE: 1,182 KM  
1,178 KM 01:38 AGO 15 KM IN 00:07

**AIRCRAFT DETAILS**

TYPE (B738)  
**Boeing 737-8MA**

REGISTRATION	MODE-S CODE
<b>VQ-BTD</b>	<b>4243CA</b>
SERIAL NUMBER (MSN)	AGE

**FLIGHT DETAILS**

GROUND SPEED TRUE AIR SPEED

The map shows the flight path of PBD156 (red arrow) and other aircraft (yellow icons) near Moscow. Key locations include Zelenograd, Dolgoprudny, and Moscow.

ADS-B

# Программно определяемое радио – SDR пример сервиса:



· [Магазин](#) · [Объявления](#) · [Рейтинг](#) · [Диапазоны](#) · [Частоты](#) · [Копилка](#) · [Форум](#)  
· [Файлы](#) · [Статьи](#) · [Сигналы](#) · [Музей](#) · [Mods](#) · [LPD-форум](#) · [Клуб](#) · [Радиостанции](#)

· [Статистика](#) · [Правила](#) · [FAQ](#) · [Создать трансляцию](#) ·

Введите ключ доступа

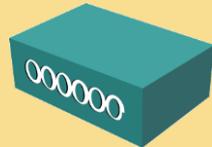


Тип	Местонахождение, название и описание трансляции	Слушают сейчас	Было макс.
	Санкт-Петербург. ULLI (LED). Международный аэропорт Пулково. ULLI: Руление Старт Круг Подход Контроль Транзит Район. Управление воздушным движением в реальном времени	10	29
	Иркутск. UIII. Иркутский авиаузел. Иркутский авиаузел – вышка, круг, руление, подход, контроль, транзит	3	5
	Краснодар. URKK. Авиадиапазон над городом. Пашковский: Подход Вышка Старт Транзит Район. Ростов-контроль.	1	73
	Москва. UUEE (SVO). Международный аэропорт Шереметьево. UUEE. Шереметьево Старт-Посадка. Транзит. АФЛ-Контроль - Левый канал. Москва Подход 2 и 5. Трансаэро контроль. Сибирь контроль. - Правый канал.	9	45
	Москва. Москва-подход M4 и M7. Внуково-подход 2. M4M7 UUMO TWR UUWW APP2	0	7
	Москва. UUEE (SVO). Международный аэропорт Шереметьево. UUEE. Шереметьево круг. Шереметьево старт - посадка.	0	7
	Москва. M1M6 UDD TWR UUWW APP 1 Подход 1,6, Домодедово-вышка, Внуково-подход 1	0	6
	Московская область. Поездная радиосвязь ПРС в г. Королёв и его окрестностях	0	3
	Новосибирск. (UNNT) Толмачево. Руление, Старт, Круг, Подход, Контроль, Транзит.	3	8
	Москва. M3M8M9 UDD APP Москва-подход-3,8,9, Домодедово-подход	0	5
	г. Королёв. Поездная связь Москвы и области Москва-Софрино, Москва-Фряезово, Казанский вокзал и проч.	2	3

# Протокол CAPWAP

Что было до SDN?

2003/ Aerospace/ Боб О'Хара/ LWAPP

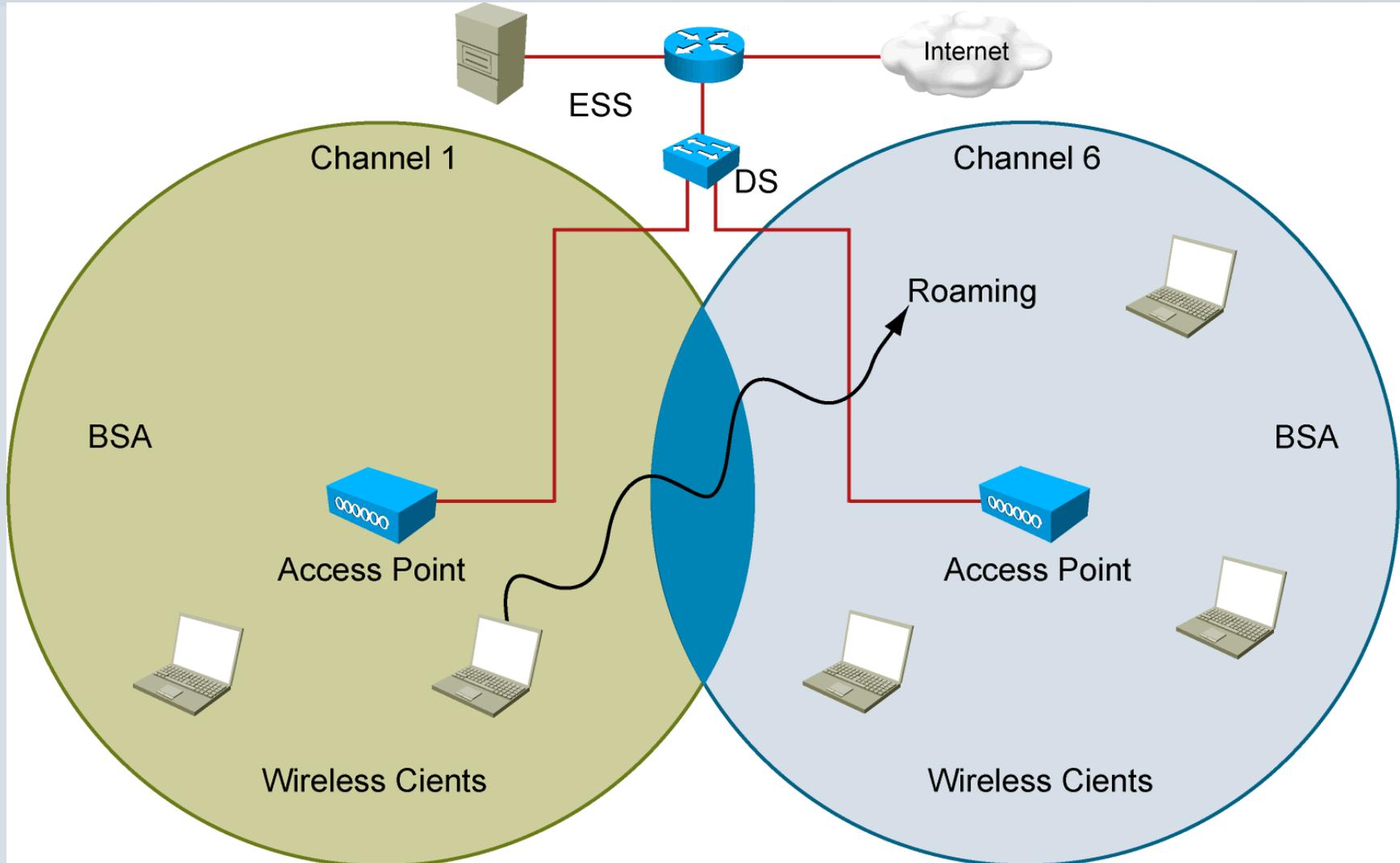


- Autonomous WLAN  
Autonomous точки доступа



- Централизованный WLAN
  - «Легкие» точки доступа
  - WLAN контроллер

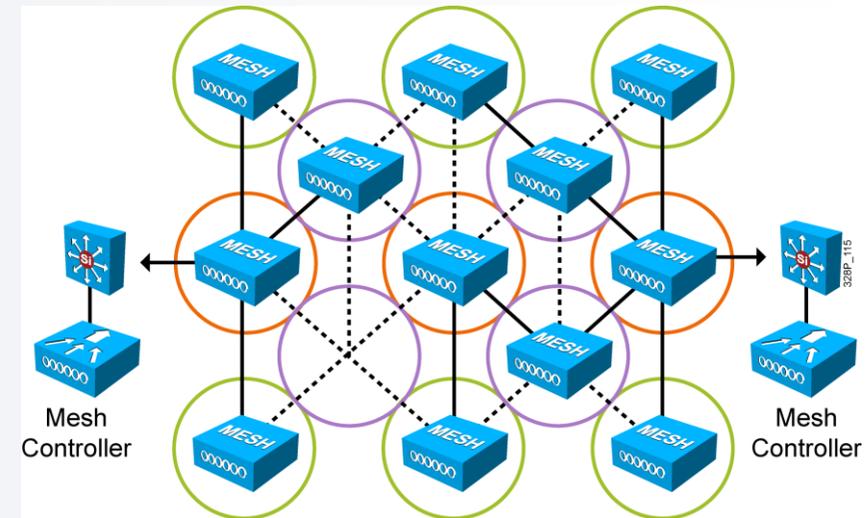
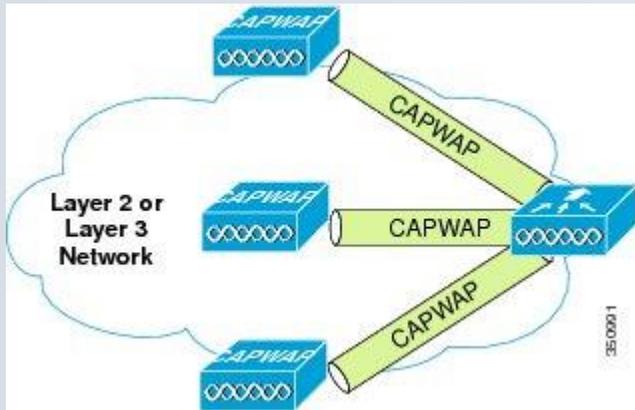
# Протокол CAPWAP



Автономные точки доступа:

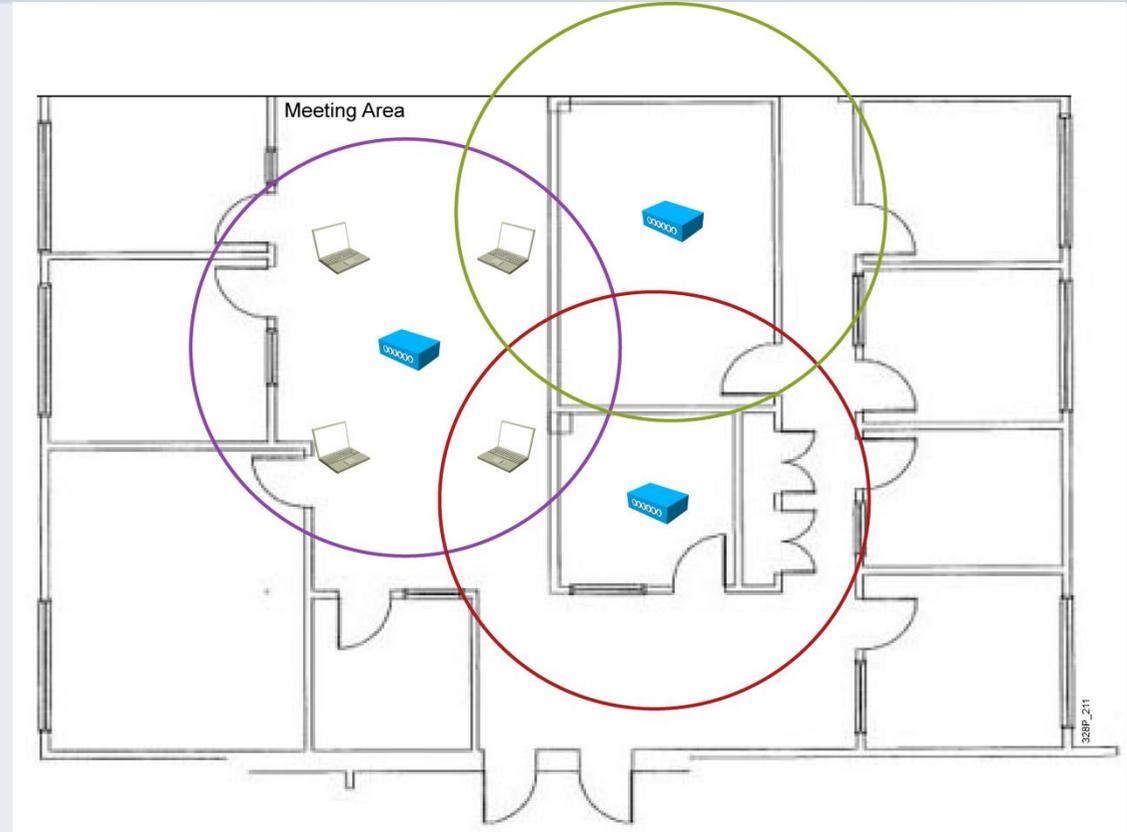
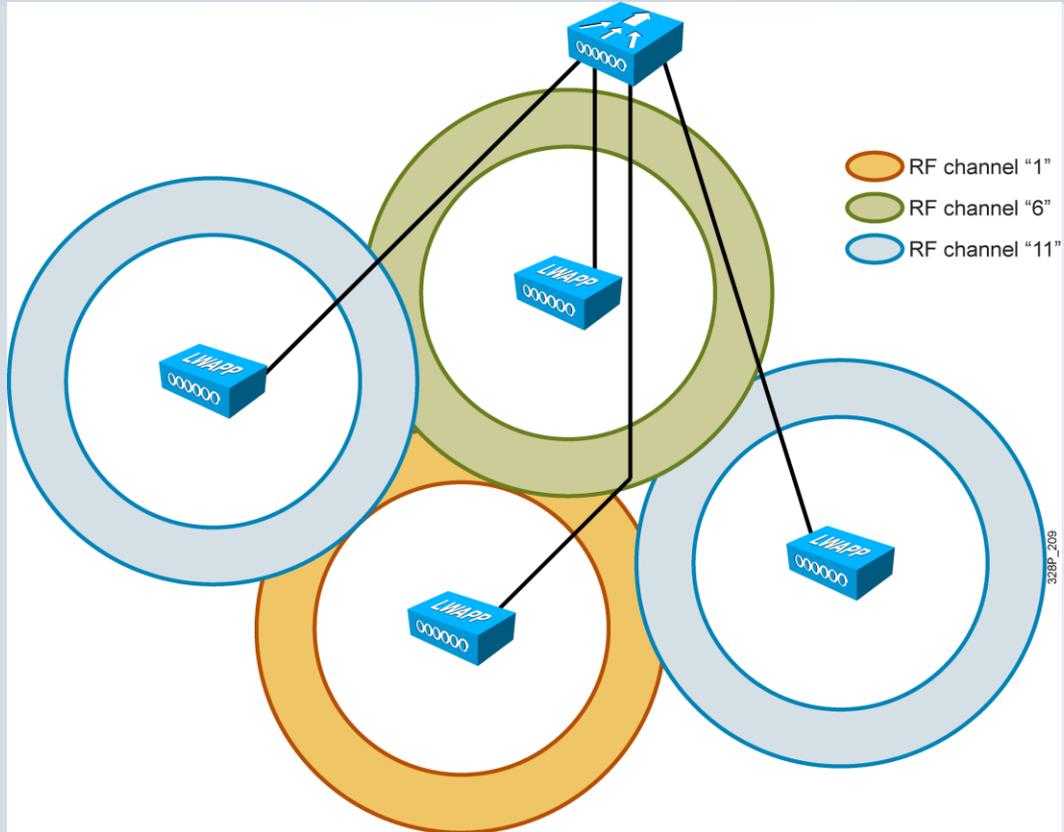
- проблемы RRM,
- работа с клиентами,
- враги
- покрытие и т.д.

# Протокол CAPWAP



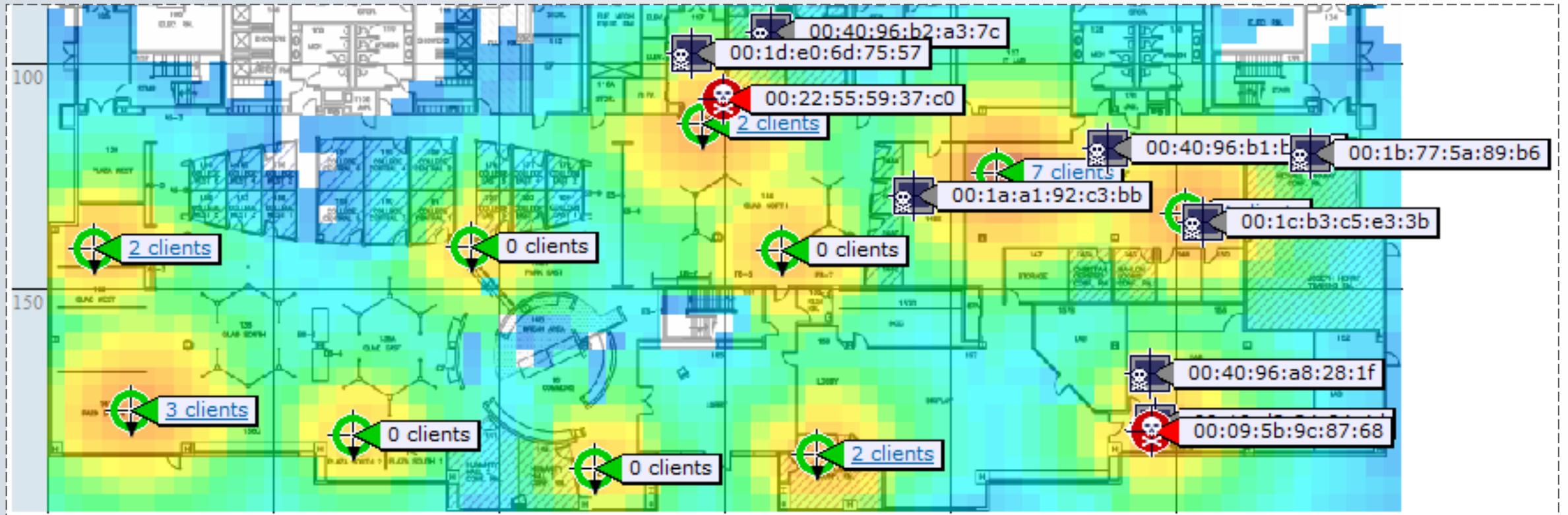
Меняется логика принятия решения: почти все решается на контроллере.  
Через несколько лет это назовут SDN.

# Протокол CAPWAP



Авто RRM, балансировка нагрузки, безопасность, Гео-сервисы, карты, планировщики, авто конфиг...

# Протокол CAPWAP

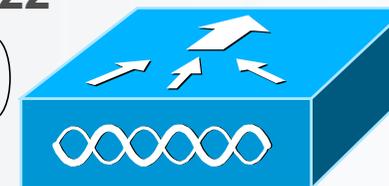
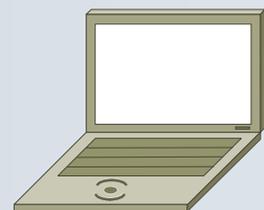


Интеграция с системами позиционирования, определение положения объекта на карте

# Протокол CAPWAP

Протокол LWAPP, разработан специально для работы точек доступа с контроллером

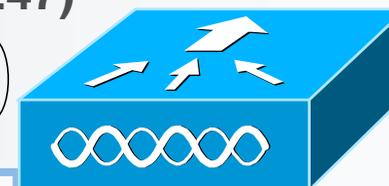
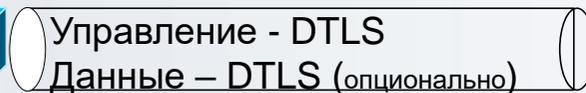
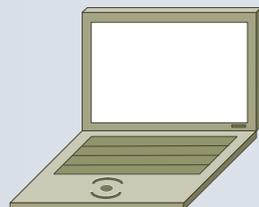
LWAPP Tunnel (Ethernet type 0xBBB, UDP 12222-12223)



LWAPP может быть L2 или L3  
Взаимная аутентификация —X.509

Протокол CAPWAP, разработан для работы точек доступа не только WiFi (RFC5415)

CAPWAP Tunnel (UDP 5246, 5247)



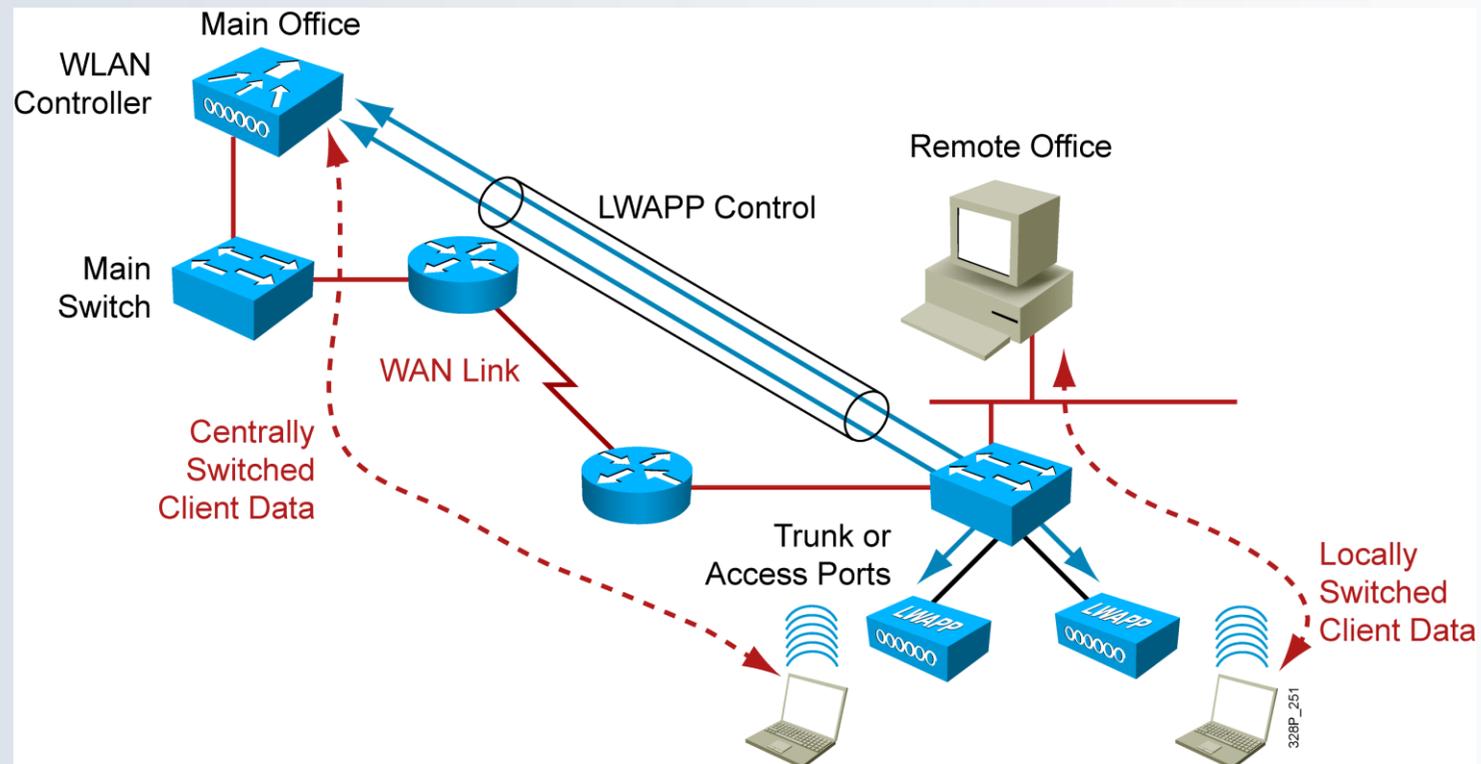
CAPWAP может быть только L3  
Взаимная аутентификация —X.509  
Возможна парольная аутентификация

...SIAPP etc.



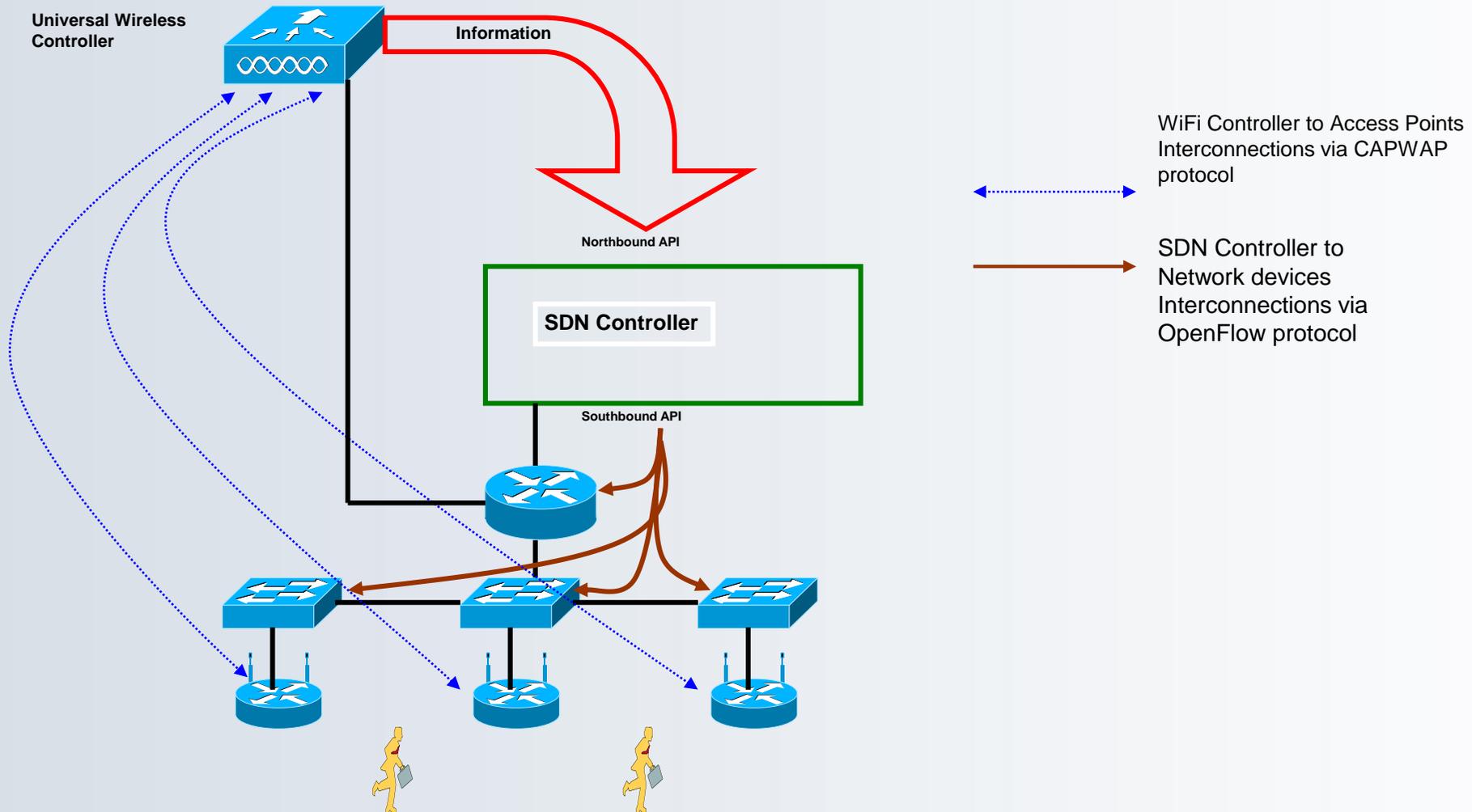
# Протокол CAPWAP

Два режима работы протокола: Split-MAC vs Local MAC



# Протокол CAPWAP

## Интеграция с ПКС сетями



# Протокол CAPWAP

Преимущества интегрированных решений capwap контроллер + SDN сеть:

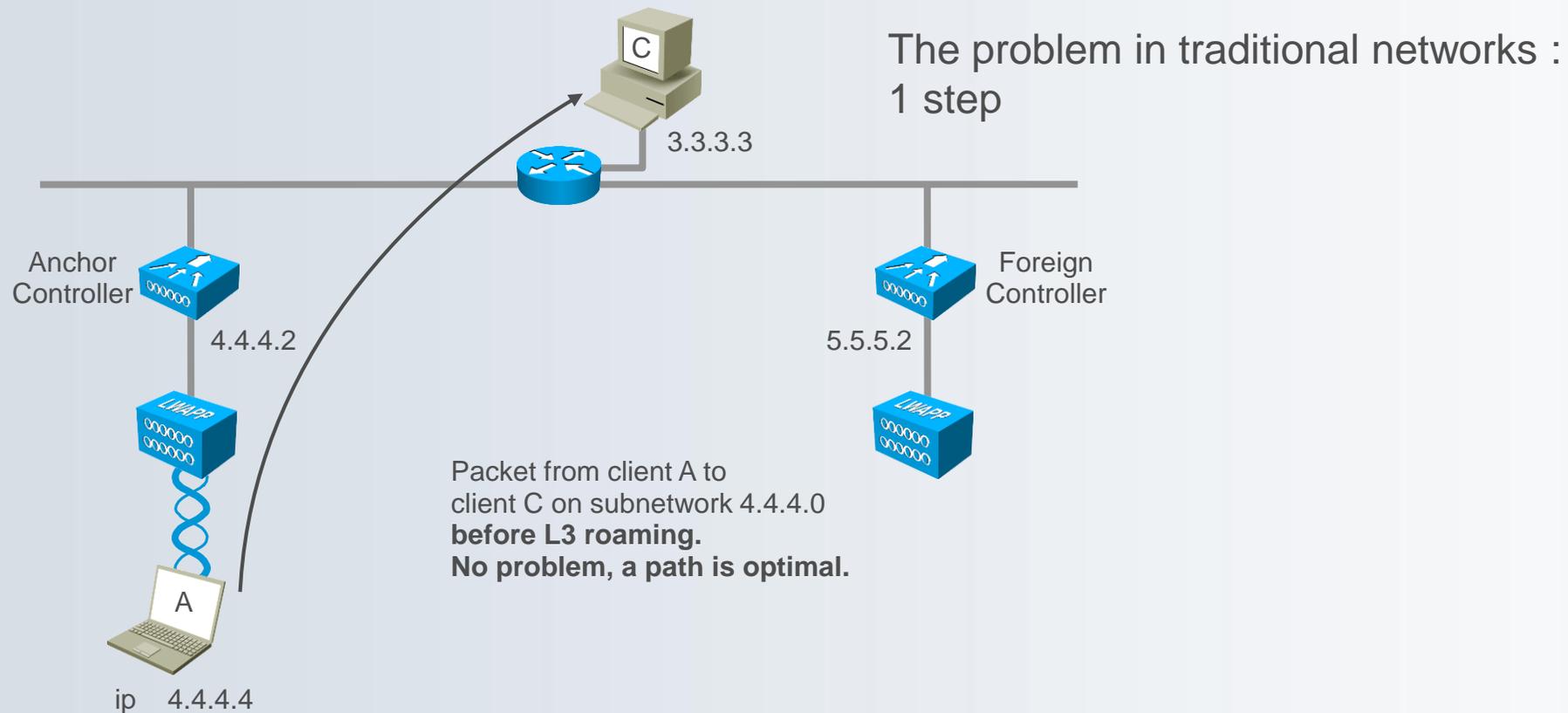
- Seamless roaming
- No excess tunnels
- Optimal paths (no excess hops)
- Ability to implement convenient geoservices

WiFi controller informs about location of user and an application configures ALL network devices for traffic of this user.

# Протокол CAPWAP

Seamless roaming – extra tunneling problem:

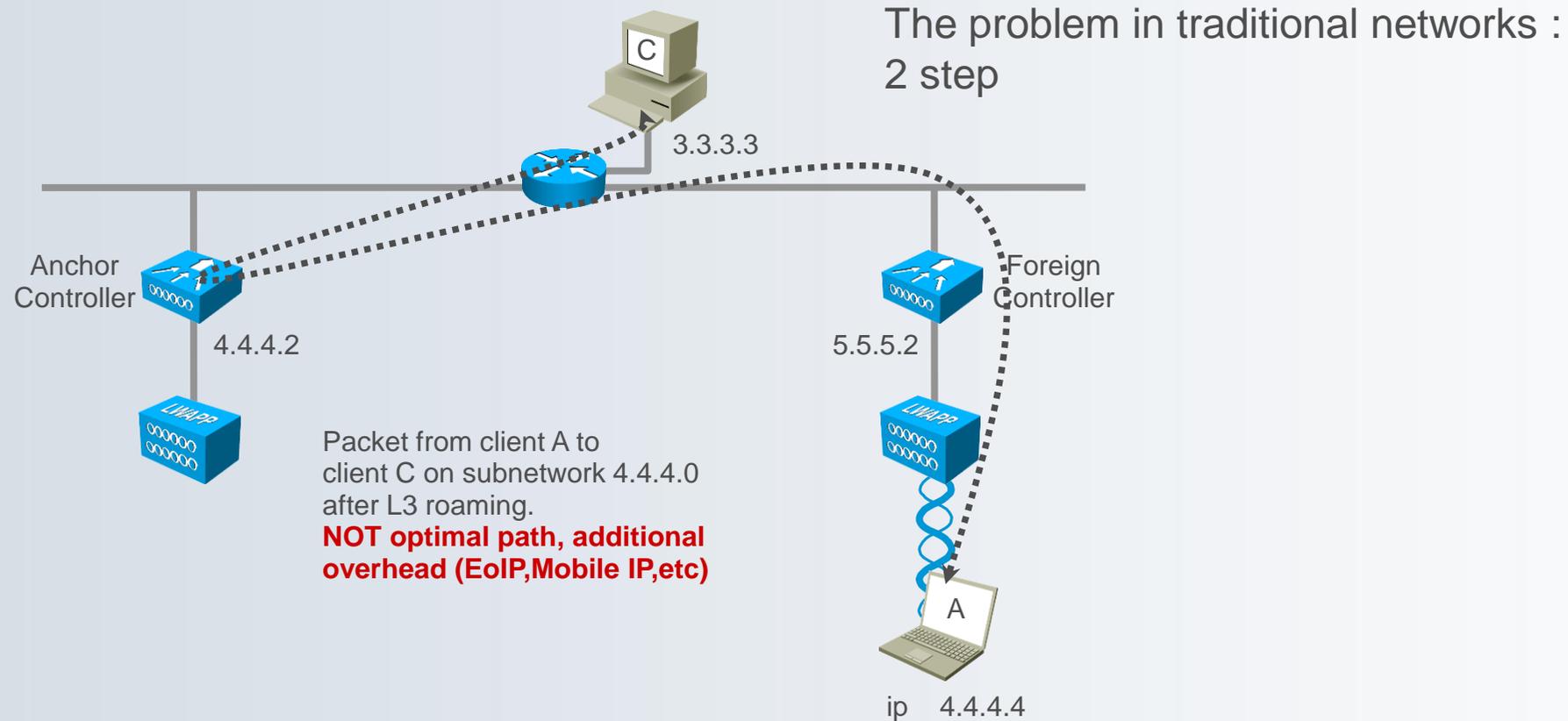
Eliminates the problem of excess tunneling Mobile IP, EthernetOverIP, etc.



# Протокол CAPWAP

Seamless roaming – extra tunneling problem:

Eliminates the problem of excess tunneling Mobile IP, EthernetOverIP, etc.

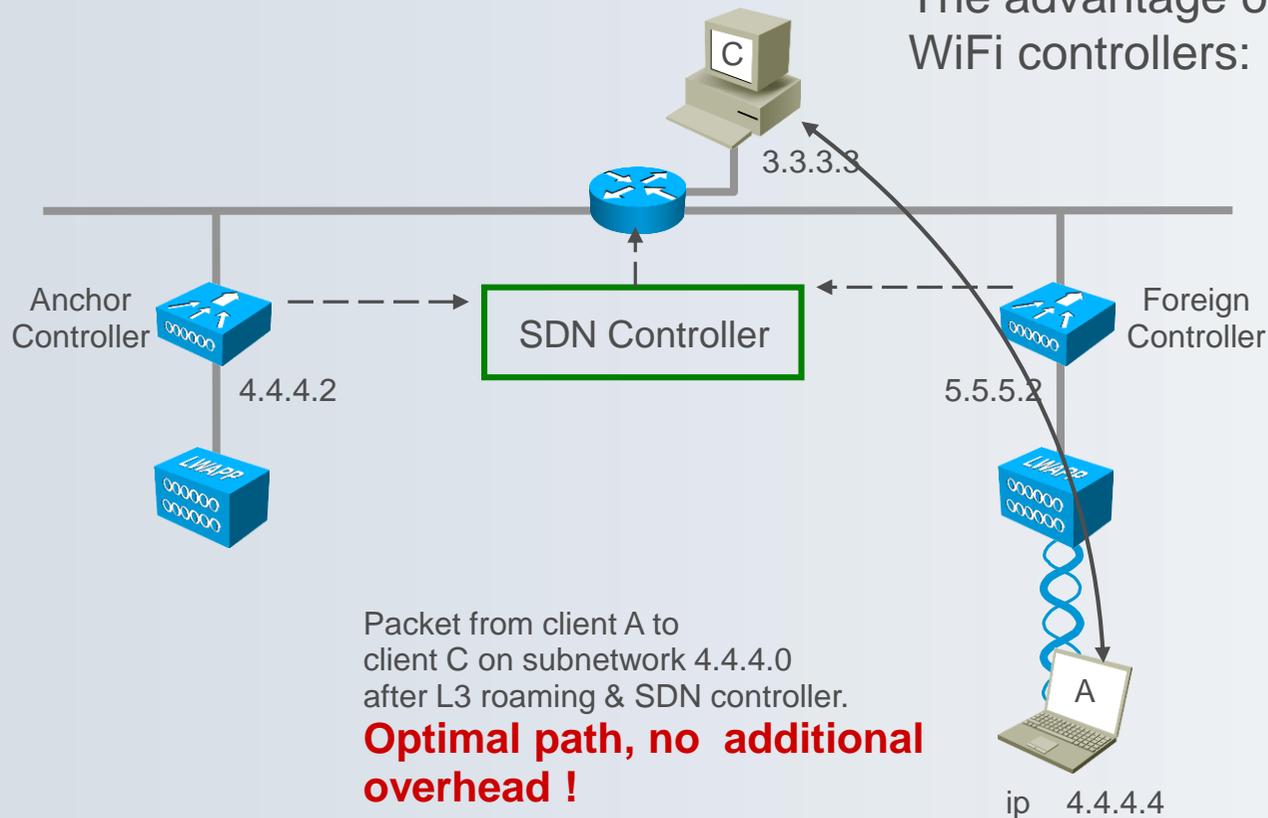


# Протокол CAPWAP

Seamless roaming – extra tunneling problem:

Eliminates the problem of excess tunneling Mobile IP, EthernetOverIP, etc.

The advantage of the integration and SDN WiFi controllers:



# Протокол CAPWAP



# Протокол CAPWAP

Дополнительные преимущества интеграции :

**Load balancing:** If the user has both wired and wireless interfaces, it allows you to balance traffic between them - SDN network will ready for it (802.11ac wave2 provide 6.9Gb/s).

**IDS and FW integrations:** If the wifi controller detects the user's actions as destructive, it will be possible to block user traffic and into wires .  
When roaming happens, the client session's context is passed to the application «Firewall» with noticing about changing of ports from where traffic is occurs.

**Geoservices:** If oblige users corporate network ALWAYS keep the wifi interface, even working through the wire, we will always know his location in the office (3-5m.) Thus we will be able dynamically change the rules, based on the geographical location!  
For example: financial documents will be accepted from the laptop only if it is in accounting room.



ЦЕНТР  
ПРИКЛАДНЫХ  
ИССЛЕДОВАНИЙ  
КОМПЬЮТЕРНЫХ  
СЕТЕЙ

[arccn.ru](http://arccn.ru)

[@ArccnNews](https://twitter.com/ArccnNews)

[smonin@arccn.ru](mailto:smonin@arccn.ru)