



# Беспроводные сети



# План

- 1. Цели
- 2. Виды беспроводных сетей
  - WiMAX
  - Bluetooth
  - GPRS сети
  - 3G сети
- 3. Категории беспроводных сетей
- 4. Способы защиты беспроводных сетей
  - Контроль доступа
  - Шифрование при помощи WEP
  - Протокол 802.1x
  - Протокол Wi-Fi Protected Access – WPA
- 5. Пример системы в Cisco Packet Tracer

# Цели

- Ознакомиться с видами беспроводных сетей и различием между ними
- Ознакомиться с основными понятиями беспроводной сети и методами ее защиты.
- Углубить свои знания о сетях



# Виды сетей:

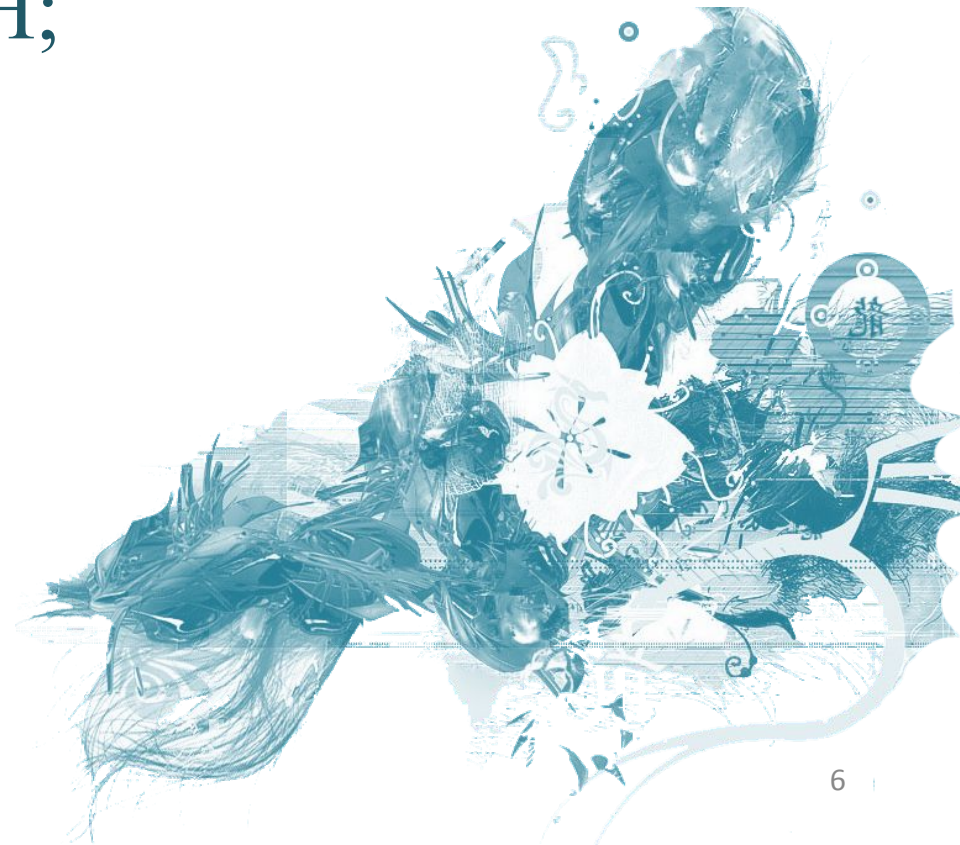
- **Традиционные проводные сети:** Данные передаются по витой паре, коаксиальному кабелю, оптоволокну и пр. Требуют затрат на прокладку кабеля
- **Беспроводные сети:** Данные передаются по воздуху, и сигнал для приема доступен для мобильных пользователей

# Сферы применения беспроводных сетей

1. Складские помещения и фабрики
2. Больницы
3. Выставочные комплексы и конференц-залы
4. Доступ к Интернет в гостиницах, кафе, библиотеках
5. «Гостевой» доступ к корпоративной сети для клиентов и партнеров
6. Сети провайдеров Интернет: подключение клиентов там, где нет возможности протянуть кабель

# Виды беспроводных сетей:

1. WI-FI И WiMAX (4G);
2. BLUETOOTH;
3. GPRS сети;
4. 3G сети.





- **Wi-Fi** – это логотип, который организация WESA (Wireless Ethernet Compatibility Alliance) использует для обозначения совместимости конкретного изделия с сетями WLAN.
- Термин возник как игра слов с Hi-Fi и никак не расшифровывается



## WiMAX —

телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств. Основана на стандарте IEEE 802.16, который также называют Wireless.

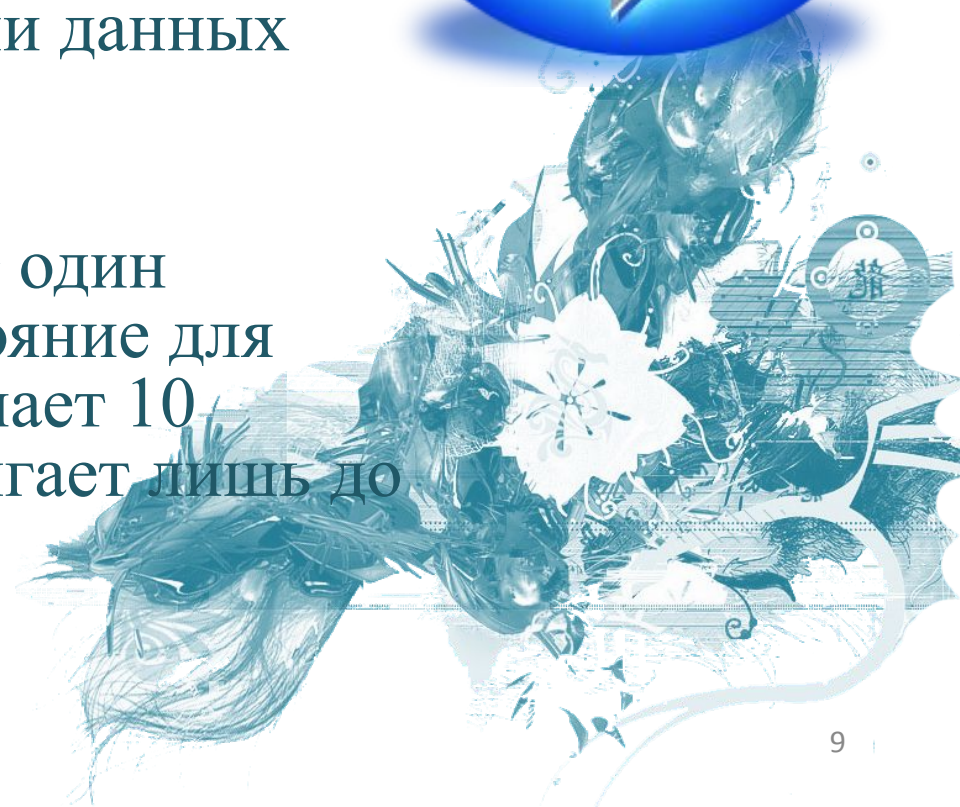
**WiMAX** Теоретически зона покрытия составляет 60 километров, на практике около 10 км. Скорость достигает 20 Мбит/сек.



# BLUETOOTH

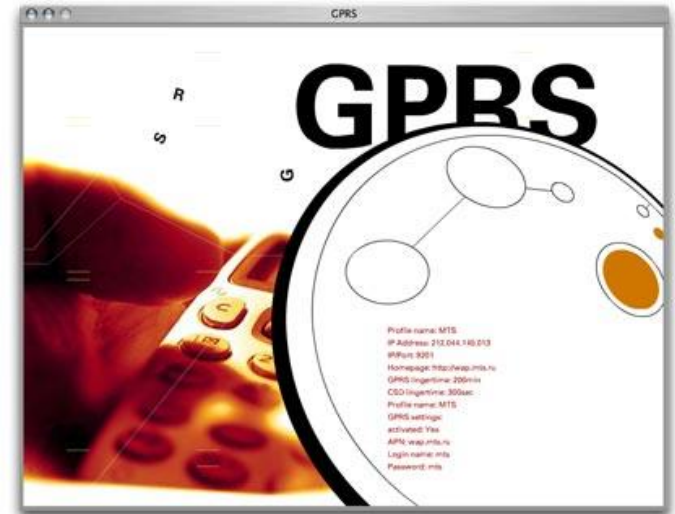


- Этот вид беспроводных сетей является самым распространенным .  
BLUETOOTH используют не только пользователи ПК. Мобильные телефоны обладают функцией передачи данных через BLUETOOTH канал.
- У BLUETOOTH существует один значительный минус. Расстояние для передачи данных не превышает 10 метров. Да и скорость достигает лишь до 100Кб/сек.



# GPRS СЕТИ

- В настоящее время в Украине действует самый медленный стандарт GPRS.
- Скорость передачи данных доходит до 100Кбсек. На данный момент GPRS используют только в Украине во всем мире отдают предпочтение 3G сетям.





## 3G сети

Изначально 3G сети использовали военные, простому населению стала доступна совсем недавно. 3G сети значительно обходят GPRS по скорости и качеству сигнала. Трафик в сетях 3G достигает 89 Мбит/сек.



# Категории беспроводных сетей

Тип	Сфера действия	Стандарты	Область применения
Персональная беспроводная сеть	В непосредственной близости от пользователя	Bluetooth, IEEE 802.15, IRDA	Замена кабелей периферийных устройств
Локальные беспроводные сети	В пределах зданий и кампусов	IEEE 802.15, Wi-Fi, HiperLAN	Мобильные расширения проводных сетей
Региональные беспроводные сети	В пределах города	IEEE 802.16, WIMAX	Фиксированная беспроводная связь между зданиями, предприятиями и Internet
Глобальные беспроводные сети	По всему миру	Сотовые системы телефонной связи поколений 2, 2.5, 3, GPRS	Мобильный доступ к Internet вне помещений

# Способы защиты беспроводных сетей

- ✓ Контроль за подключением к точке доступа на основе MAC-адресов и имени сети
- ✓ Шифрование на основе протокола WEP<sup>®</sup> (RC4)
- ✓ Контроль за доступом к среде передачи на основе протокола 802.1x
- ✓ Поддержка нового протокола WPA (AES)

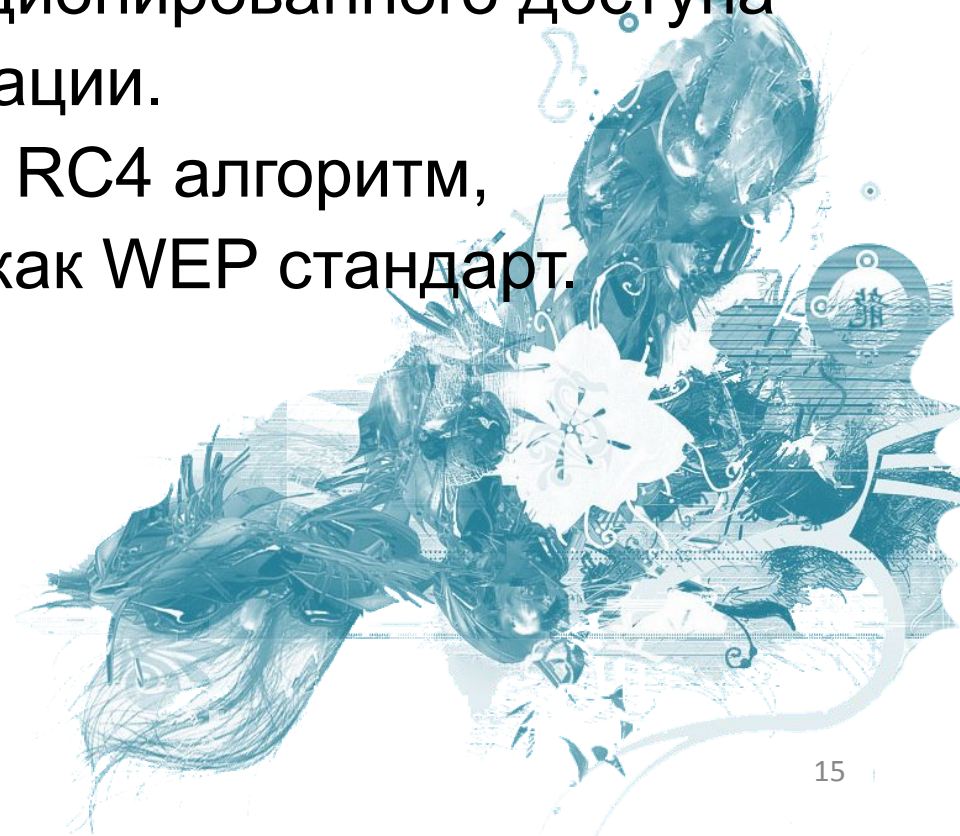
# Контроль доступа

- *По имени сети:* Вы можете использовать уникальный ESSID во избежание несанкционированного доступа в Вашу беспроводную сеть
- *По MAC-адресу:* Вы можете задать на точке доступа список MAC-адресов, которым Вы хотите разрешить авторизацию в Вашей группе в сети на Вашей точке доступа.

# Шифрование при помощи WEP

Вы можете включить на всех беспроводных устройствах шифрование всего трафика для предотвращения несанкционированного доступа к передаваемой информации.

Шифрование использует RC4 алгоритм, принятый в IEEE 802.11 как WEP стандарт.



# Протокол 802.1x

**Для аутентификации и авторизации пользователей с последующим предоставлением им доступа к среде передачи данных, разработан стандарт безопасности IEEE 802.1x, который ориентирован на все виды сетей доступа, соответствующие стандартам IEEE.**

**Данная система предназначена для совместной работы EAP (Extensive Authentication Protocol) и RADIUS.**

**Прежде чем получить доступ к беспроводной (или проводной) сети, клиент должен пройти проверку на сервере RADIUS и только в случае успешной проверки ему разрешается доступ в сеть.**



# Протокол Wi-Fi Protected Access - WPA

Для замены протокола WEP Wi-Fi была разработана новая система безопасности – WPA.

**Основные достоинства WPA:**

- Более надежный механизм шифрования, основанный на «временном протоколе целостности ключей» - Temporal Key Integrity Protocol (TKIP)
- Аутентификация пользователей при помощи 802.1x и EAP
- Совместимость с будущим протоколом безопасности беспроводных сетей 802.11i
- Возможность работы в сетях класса SOHO без необходимости настройки сервера RADIUS – режим Pre-Shared Key (PSK), позволяющий вручную задавать ключи

# Пример системы в Cisco Packet Tracer

The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a central 2621XM Router0 connected to five cloud-based peers (Peer0 to Peer5) and a PC-PT InstrHost. The connections are shown as red lightning bolts. The interface includes a menu bar (File, Edit, Options, View, Tools, Extensions, Help), a toolbar, and a status bar at the bottom. The status bar shows the time as 00:01:01 and the Realtime mode. The bottom panel contains a 'Routers' palette with various models (1841, 2620XM, 2621XM, 2811, Generic) and a 'Scenario 0' dropdown menu. The right sidebar contains a 'To use:' section with instructions and a list of peer information.

**To use:**

Ensure that the MU\_RIP\_Instructor... that all student devices can reach th

Instructor cloud information should k  
Connection type: incoming  
password: cisco

Student peer information should look  
connection type: outgoing  
local host: 38000  
peer name: peer# (# based on whic  
password: cisco

Once students try to connect, a "cor  
to accept the connection. If cloud dc  
connection between router0 and pee

Peer0 - S0/0 (10.1.\_.0/24)  
Peer1 - S0/1 (10.10.\_.0/24)  
Peer2 - S0/2 (10.20.\_.0/24)  
Peer3 - S0/3 (10.30.\_.0/24)  
Peer4 - S1/0 (10.40.\_.0/24)  
Peer5 - S1/1 (10.50.\_.0/24)

One student enable FIG00 101...

СПАСИБО

ЗА

ВНИМАНИЕ

