Министерство образования Республики Беларусь
Учреждение образования
Гомельский государственный университет им. Ф. Скорины

Физический факультет

«Информационные системы и сети»

Лекция – Безопасность в беспроводных сетях

Лектор – ст. преподаватель Грищенко В.В.

Безопасность в беспроводных сетях

Для обеспечения безопасности в беспроводных сетях используется несколько средств:

- **Контроль за подключением к точке доступа на основе MAC-адресов и имени сети**
- **Шифрование на основе протокола WEP (RC4)**
- **Контроль за доступом к среде передачи на основе протокола 802.1x**
- **Поддержка нового протокола WPA (AES)**
- **Настройка VPN поверх беспроводного соединения**
- **Вынос беспроводной сети за межсетевой экран, как сети с низким доверием**

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, котором 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.

- **64 и 128 bit шифрование доступно для клиентов. 64 bit WEP и 40 bit WEP – это одно и то же.**
- **40 bit (10 шестнадцатеричных символов) - «секретный ключ" (устанавливается пользователем), и 24 bit - «инициализационный вектор" (не зависит от пользователя).**

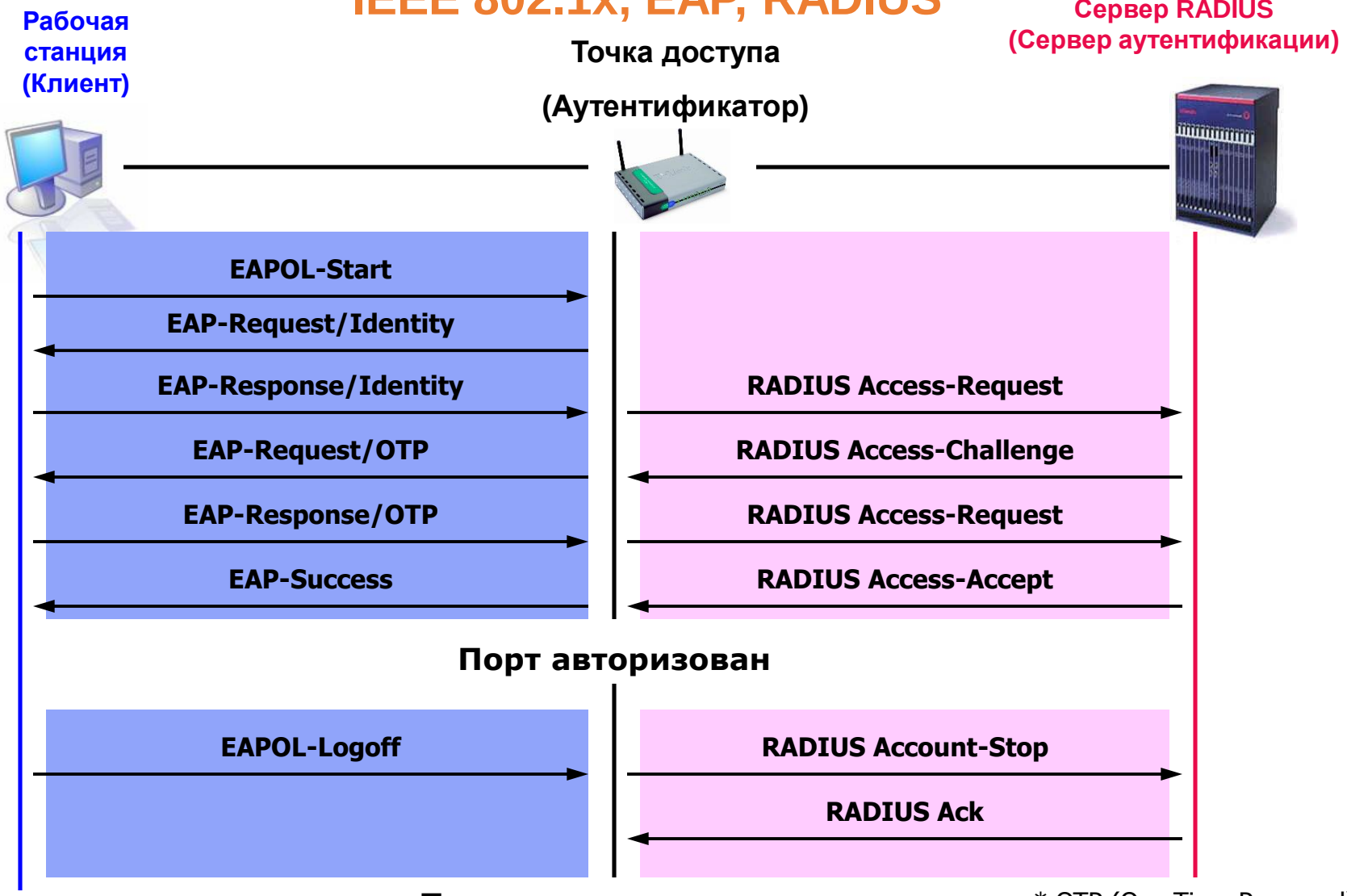
Протокол 802.1x

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 есть.

IEEE 802.1x, EAP, RADIUS



* OTP (One-Time-Password)

Протокол Wi-Fi Protected Access - WPA

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

Основные достоинства WPA:

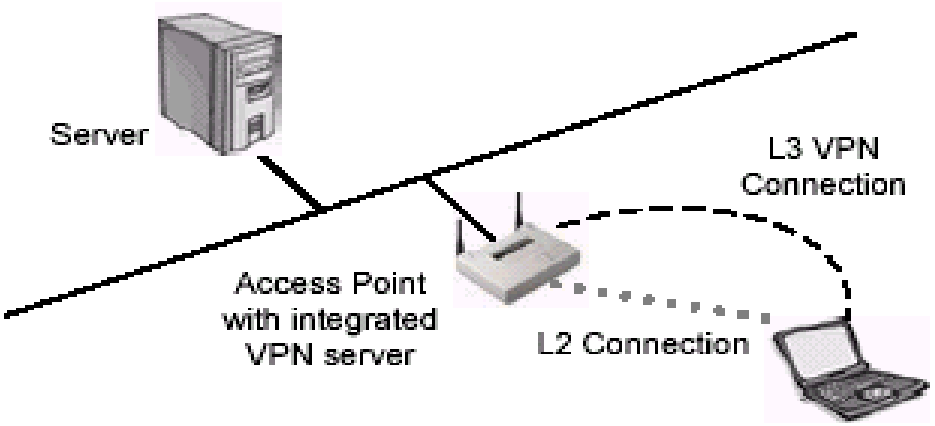
- **Более надежный механизм шифрования, основанный на «временном протоколе целостности ключей» - Temporal Key Integrity Protocol (TKIP)**
- **Аутентификация пользователей при помощи 802.1x и EAP**
- **Совместимость в с будущим протоколом безопасности беспроводных сетей 802.11i**
- **Возможность работы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

Сравнение протоколов WEP, WPA и 802.11i

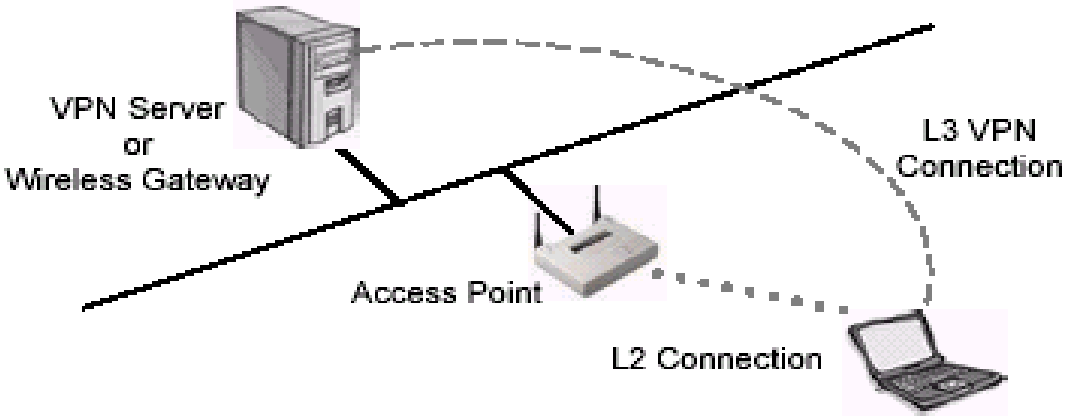
	WEP	WPA	802.11i
Шифрование	RC4	RC4	AES
Длина ключа	40/104 бита	128 бит - шифрование 64 бита - аутентификация	128 бит
Повторяемость ключа	24 битный IV	48 битный IV	48 битный IV
Целостность данных	CRC-32	Michael	CCM
Целостность заголовка	Отсутствует	Michael	CCM
Управление ключами	Статические для всей сети	На основе EAP	На основе EAP
Аутентификация	WEP ключ	IEEE 802.1x	IEEE 802.1x

Wireless и VPN

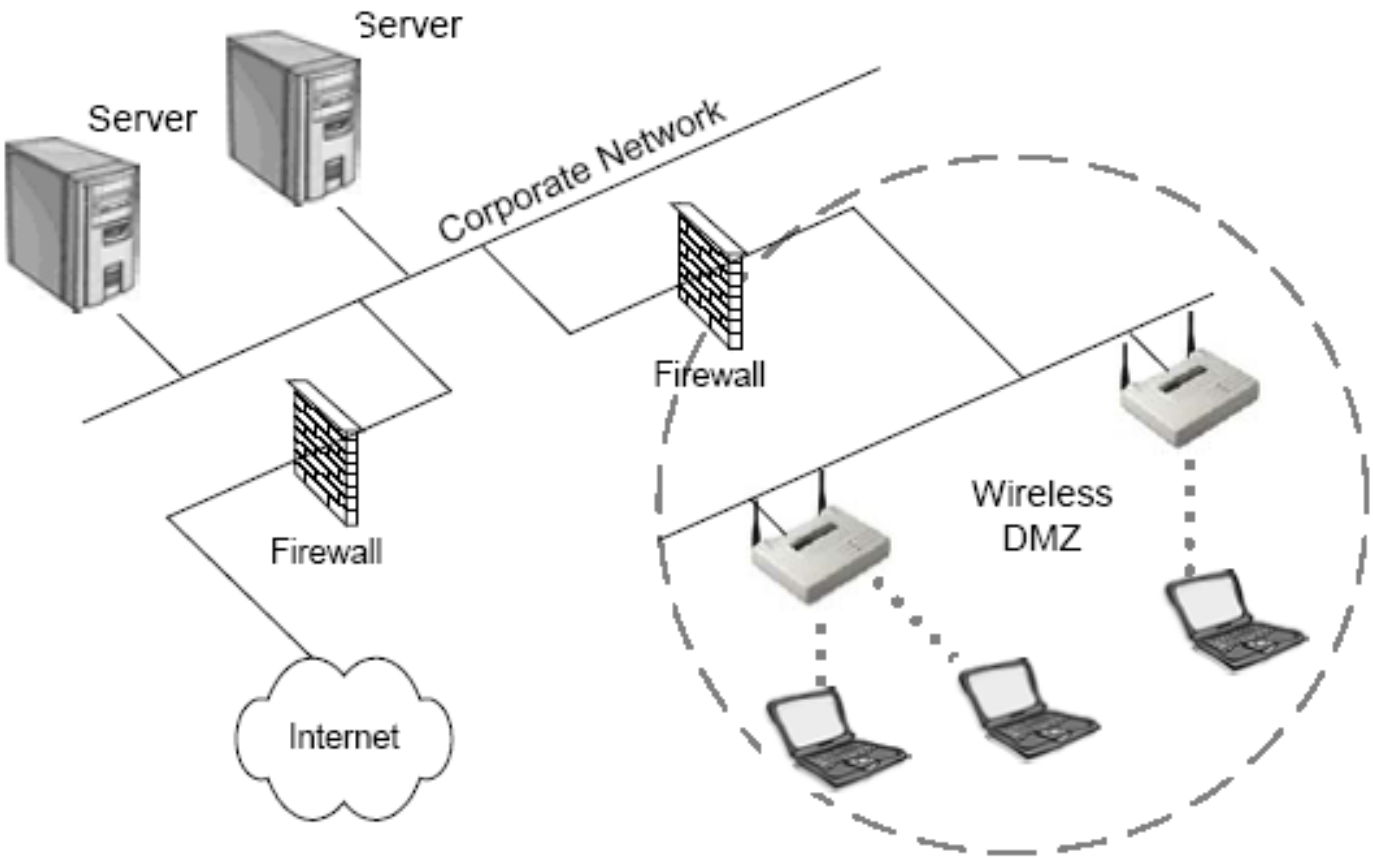
Access point with an integrated VPN server



Access point with an external VPN server



Защита при помощи межсетевого экрана



Рекомендации по обеспечению безопасности в беспроводных сетях

	Точка доступа LAN	Точка доступа HotSpot	Мост
Использование WPA	☑		
Использование 802.1x	☑		
Использование WEP	☑	☑	☑
Использование VPN			☑
Вынос точки доступа за файрвол	☑	☑	☑
Аутентификация на пограничном ресурсе	☑	☑	
Фильтрация по MAC адресам	☑		☑
Отключение SSID Broadcast	☑		☑

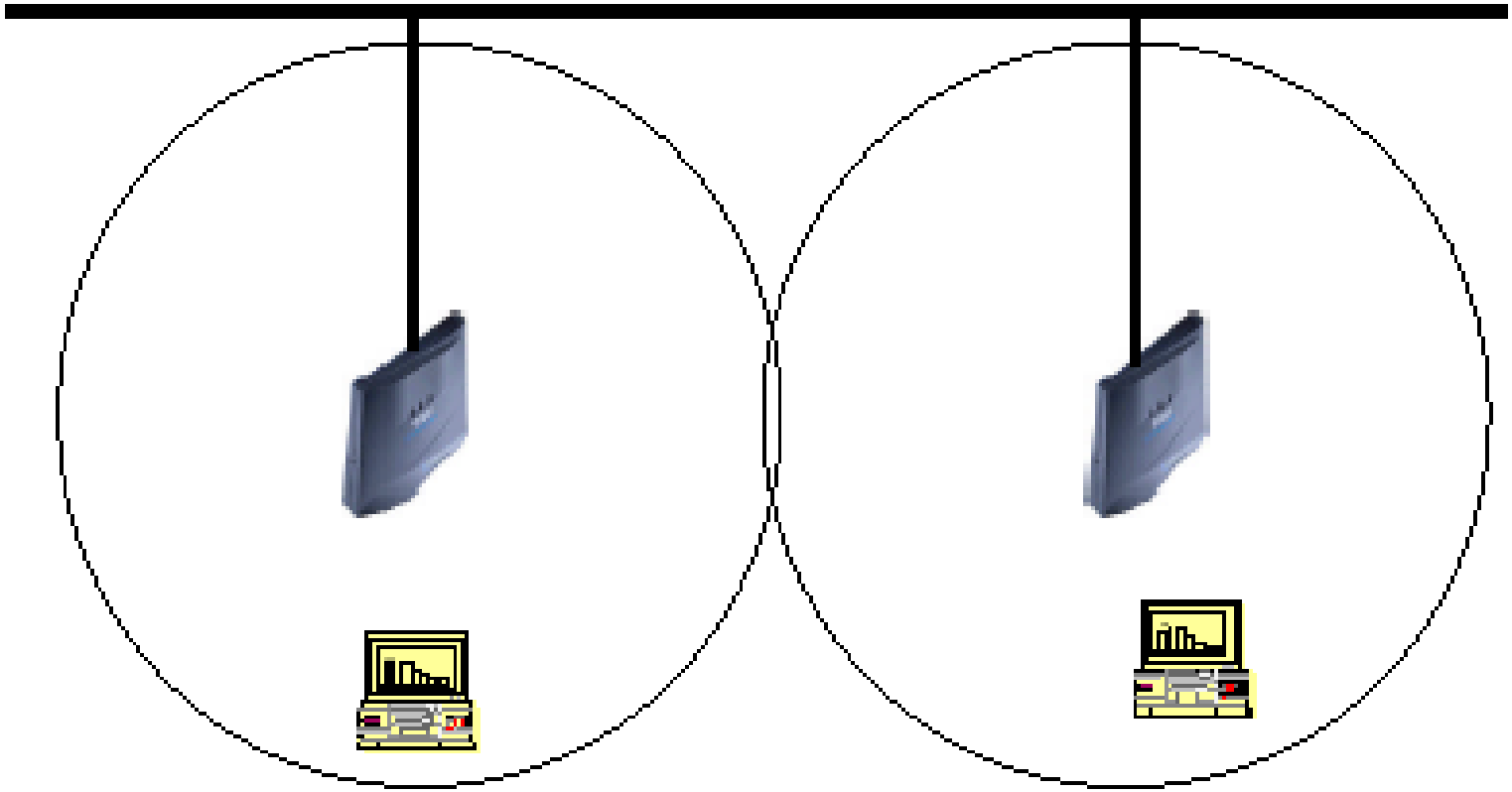
Планирование и развертывание беспроводной сети предприятия

При развертывании беспроводной сети нужно определить плотность размещения точек доступа для обеспечения роуминга и беспрерывной связи при перемещении клиентов

Необходимо разместить точки доступа так, чтобы:

- **Увеличить зону покрытия**
- **Обеспечить качество связи и необходимую пропускную способность**
- **Не допустить пересечения каналов точек доступа**

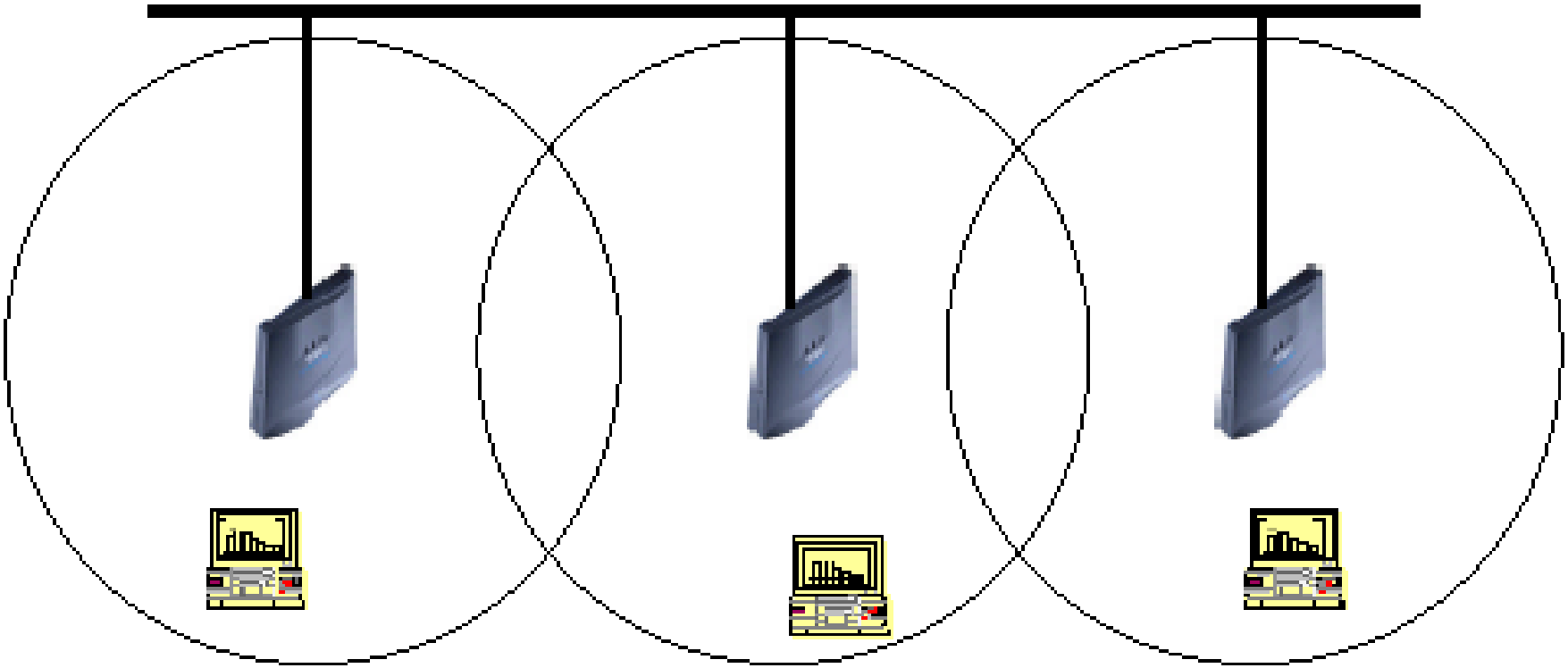
Низкая плотность - используется для покрытия большой площади наименьшим количеством точек доступа.



Средняя плотность:

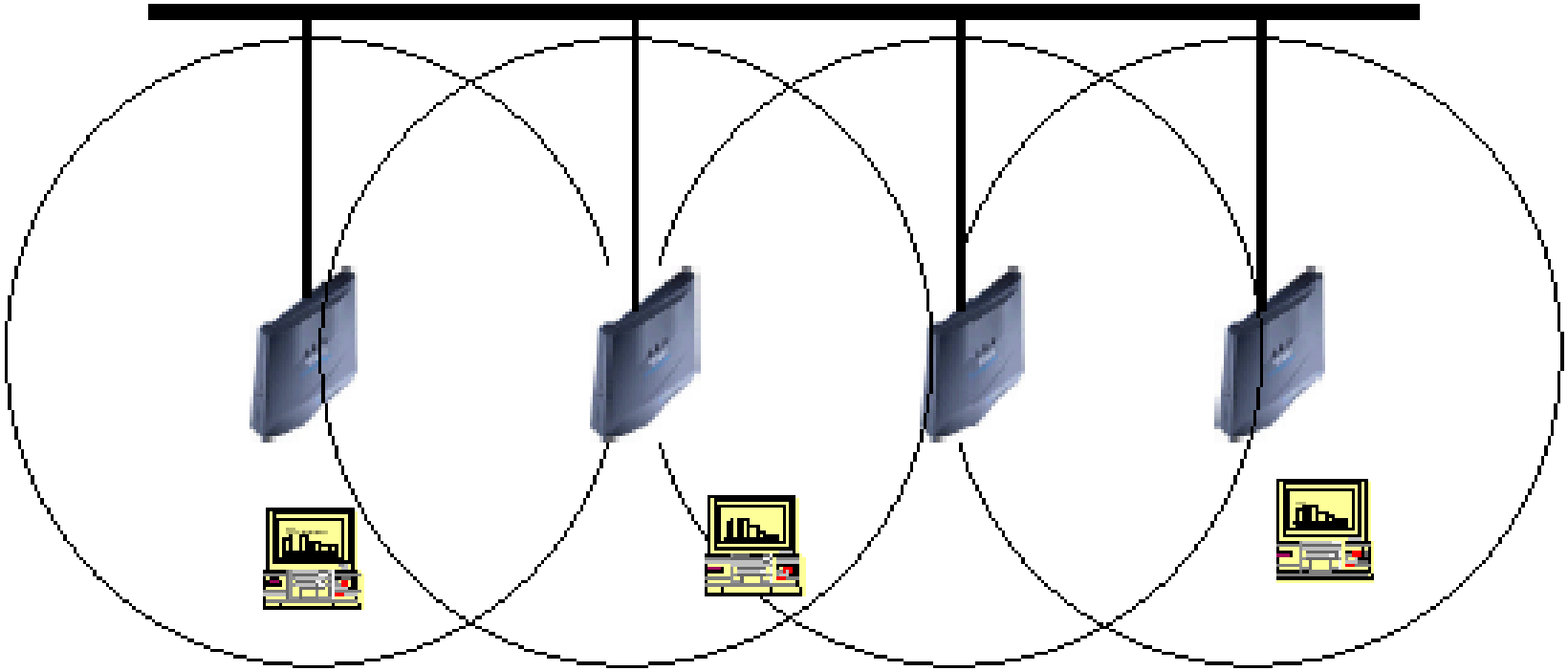
•Используется для предоставления и широкой зоны охвата и хорошей пропускной способности

•Характеризуется 20% перекрытием в зоне охвата

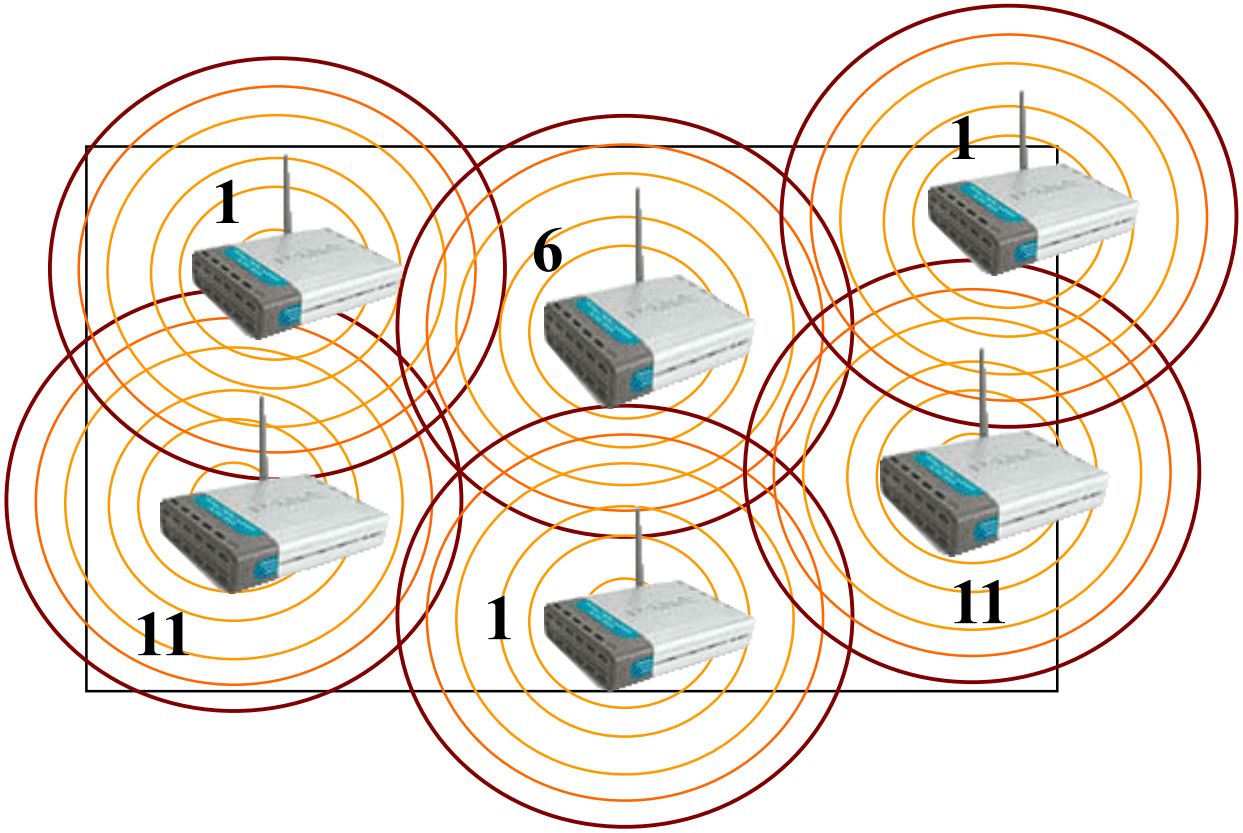


Высокая плотность

- Используется для максимальной пропускной способности
- Характеризуется примерно 50% перекрытием и использованием нескольких каналов



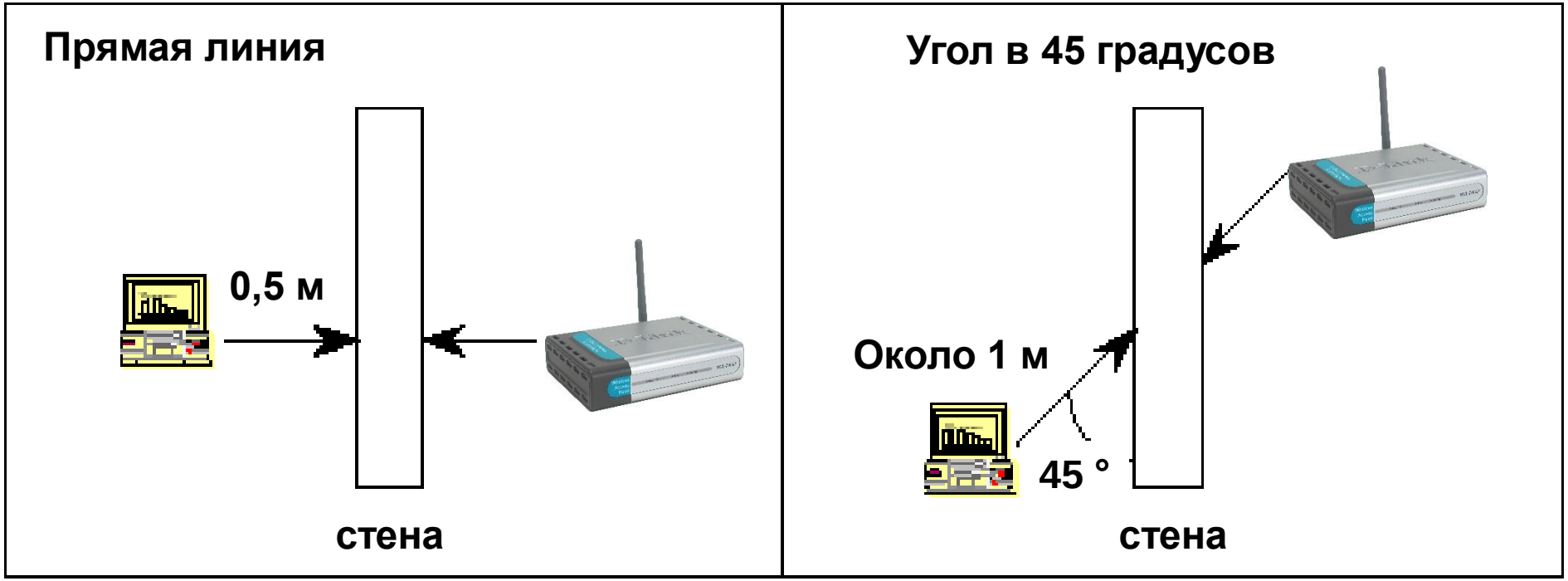
Пример расположения точек доступа и настройки каналов



При планировании беспроводной сети необходимо учитывать следующие моменты:

- Расположение Точек Доступа зависит от необходимой площади охвата и конструкции здания.
- Толстые стены, или стены с металлоконструкциями, будут блокировать сигнал сильнее, чем светопропускающие конструкции.
- Количество стен и перегородок желательно свести к минимуму – каждая стена может сокращать максимальную дистанцию для передачи данных на 1 - 30 м.

•Располагайте беспроводные устройства по прямой линии: стена толщиной в 0,5 м. При расположении устройств под углом в 45 градусов становится толщиной почти 1м.



- Офисная мебель, кабинеты, могут образовывать “тени” в зоне охвата.
- Для получения широкой зоны охвата необходима прямая видимость.
- Удостоверьтесь, что антенна настроена для лучшего приема

•Располагайте беспроводные устройства вдали (по крайней мере от 1 до 2 метров) от электрических устройств, которые генерируют радиосигнал

Возможные радиочастотные источники шума:

- Микроволновые печи
- Охранные системы (store gateways)
- Коротковолновые видео-передатчики

Возможна интерференция волн, излучаемых этими устройствами.

Некоторые типичные проблемы при проектировании беспроводной сети

Отношение сигнал - шум (SNR) хорошее, но производительность данных - относительно низкая:

- Перегруженная сеть – слишком много клиентов пытаются получить доступ к среде передачи
- Электрическое устройство, генерирующее радиосигнал, расположено рядом с беспроводным клиентом
- Качество связи другого клиента недостаточно хорошее и поэтому он возникает много повторной передачи пакетов
- Коллизии, возникающие из-за проблемы «скрытый узел»

Концентрация пользователей на точку доступа слишком высокая:

- Разместите ближе точки доступа, чтобы распределить нагрузку
- Добавьте дополнительные точки доступа к беспроводной сети

Уровень сигнала низкий:

- Устройства могут быть слишком далеко друг от друга
- Имеется преграда между устройствами

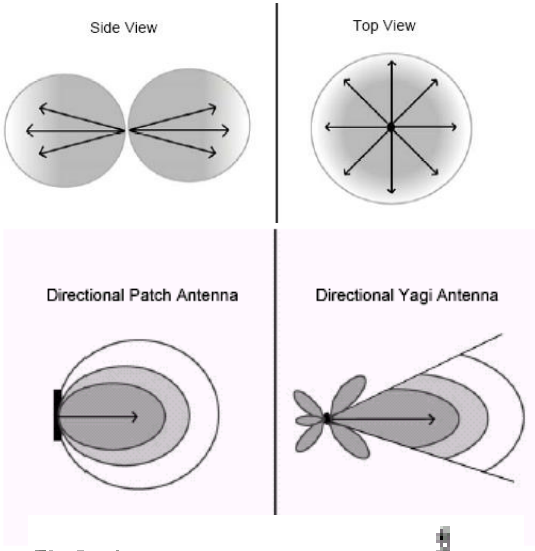
Варианты внешнего применения

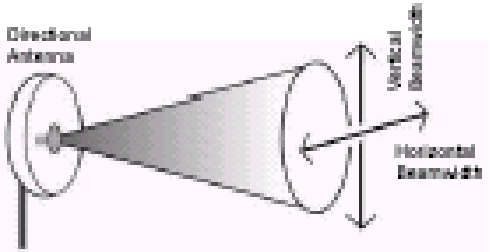
- 1. Готовые наборы от производителя (DWL-1800R/B, DWL-1700AP, DWL-1750)

- 2. Конструктор «сделай сам».
- Стационарная антенна снимается ?
- Прямая видимость между антеннами
- Кабель переходник от фирменного к N-типа стандартному
- СВЧ кабель нужной длины, разъемы N-типа
- Усилитель СВЧ сигнала
- Газоразрядник
- Антена

Типы антенн

- **Диапазон – 2,4Ггц**
- **Коэффициент усиления dBi**
- **Стандартные разъемы N-типа**
- **Направленые (directional)**
- **Полунаправленные (секторные) semi-**
- **Всенаправленные (omni-directional)**

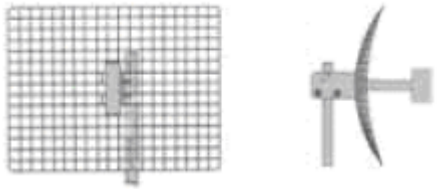




Yagi Antenna

Patch Antenna

Panel Antenna



Grid Antenna