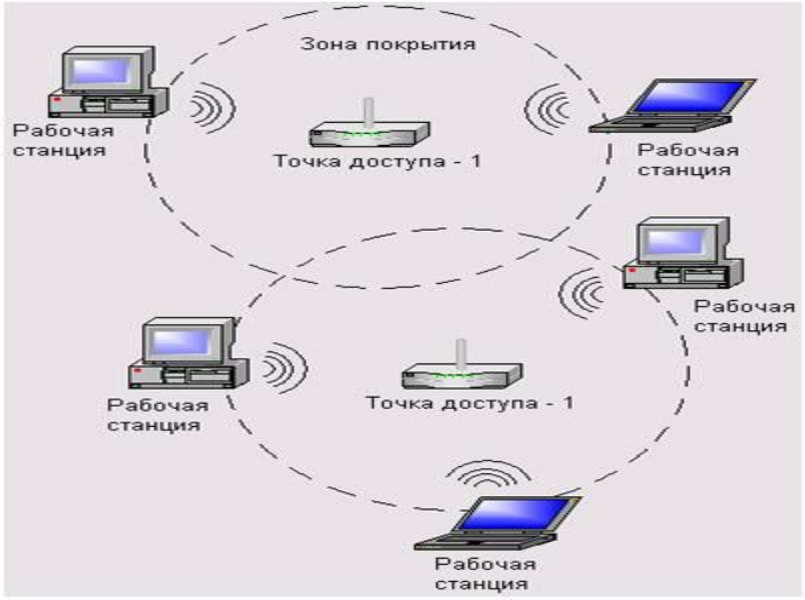
Беспроводные сети

- *Беспроводные компьютерные сети* — это технология, позволяющая создавать вычислительные сети, полностью соответствующие стандартам для обычных проводных сетей (например, Ethernet), без использования кабельной проводки.

Беспроводные сети

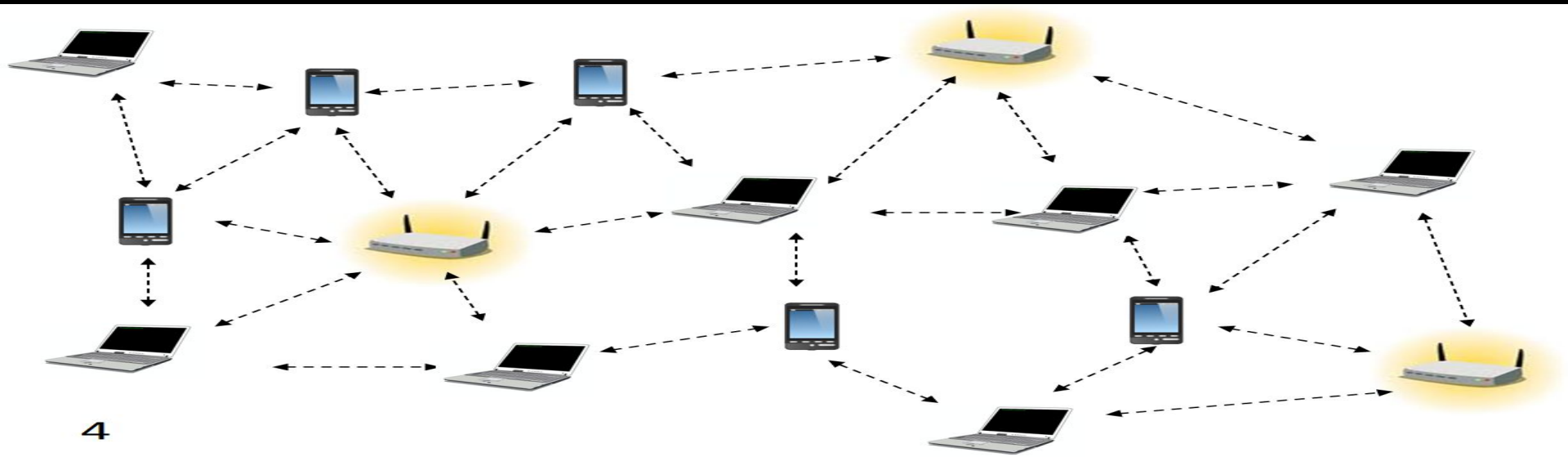


Беспроводная точка доступа

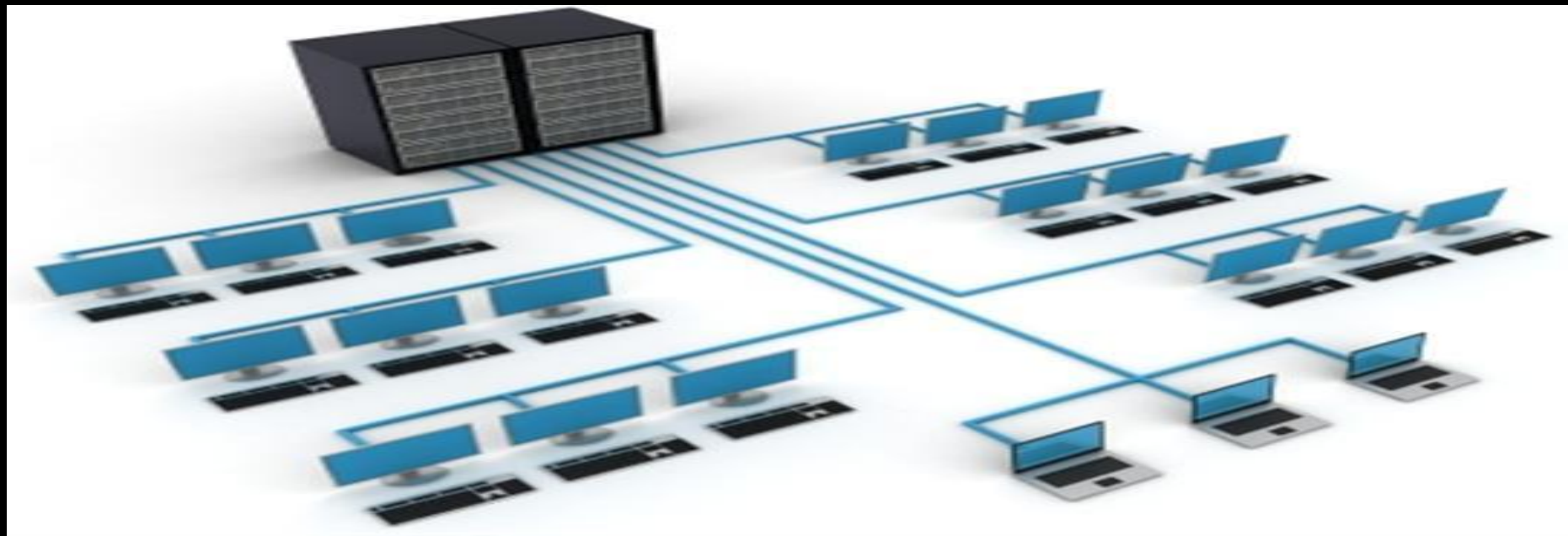
USB-адаптер

- Существуют два вида беспроводных сетей: ad-hoc и инфраструктурная сеть.

- Сеть ad-hoc(читается эд-хок) это наиболее простая беспроводная сеть, которая создается посредством объединения двух или более беспроводных клиентов без наличия точки доступа. Все клиенты внутри сети ad-hoc равноправны и позволяет организовать обмен файлами и информацией между устройствами без затрат и сложностей, связанных с приобретением и настройкой точки доступа.



- Инфраструктурная сеть– обладает точкой доступа, управляющей обменом данных в пределах беспроводной соты (зоны покрытия). Точка доступа определяет, какие узлы и в какое время могут устанавливать связь. Такой режим работы сети наиболее популярен. При такой форме организации беспроводных сетей отдельные беспроводные устройства не могут взаимодействовать между собой напрямую. Чтобы эти устройства могли взаимодействовать между собой, им необходимо разрешение от точки доступа. Точка доступа управляет всеми взаимодействиями и обеспечивает равный доступ к сети всем устройствам.
- Как было упомянуто, точка доступа имеет ограниченную зону покрытия. Для увеличения зоны покрытия, можно установить несколько точек доступа с общим SSID. В таком случае, следует помнить, что для того, чтобы переход между сотами был возможен без потери сигнала, зоны покрытия соседних точек доступа должны пересекаться между собой примерно на 10%. Это позволяет клиенту подключаться ко второй точке доступа перед тем, как отключиться от первой точки доступа.



Достоинства и недостатки использования беспроводной сети

ДОСТОИНСТВА:

- избавление от кабелей (самый большой плюс);
- минимум монтажных работ;
- могут обслуживаться места, где нельзя проложить кабель (например, в зданиях, имеющих историческую ценность);
- избавляет от привязки к конкретному месту;
- легкость переезда всего оборудования;
- позволяет иметь доступ к сети мобильным устройствам.

Недостатки

- если сеть построена или пролегает через открытое пространство (улицы, дома, Ж/Д пути и пр.) возможны помехи как от других линий связи, так и от плохой погоды (дождь, снегопад), для устранения данных помех придется докупать дополнительное оборудование;
- при незащищенном использование возможен легкий доступ извне, в радиусе действия сетей Wi-Fi. Для предотвращения этого существует шифрование канала, которое нужно обязательно использовать при создании сети;
- ну и стоимость, чаще всего, получается дороже, чем воздвигнуть проводную сеть.
- большим недостатком есть протоколы кодирования. Например, если вы пользуетесь беспроводным интернетом в общественном месте, вся ваша информация доступна третьей стороне. Все данные, включая даже те, что вы храните у себя на жестком диске ноутбука;
- из-за того, что количество пользователей беспроводного доступа с каждым днем становится больше, увеличивается и нагрузка на каналы, по которым передаются данные. Со временем, если на эту проблему не обратить должного внимания, одни пользователи будут мешать другим;
- кроме маршрутизаторов, перегружать беспроводные сети могут и другие устройства, такие как радиотелефоны, микроволновые печи (создают помехи при передаче данных), а также устройства Bluetooth. Чем больше город, тем больше возможность перегрузки сетей;
- беспроводные маршрутизаторы имеют свой диапазон работы, радиусом от 45 до 90 метров. Диапазон можно расширить, купив антенну;
- при постоянном использовании канала передачи данных, батарея вашего ноутбука будет быстрее разряжаться, чем если бы он был подключен через кабель;

Аутентификация в беспроводных сетях

Стандарт IEEE 802.11 сети с традиционной безопасностью

Стандарт IEEE 802.11 с традиционной безопасностью (Tradition Security Network - TSN) предусматривает два механизма аутентификации беспроводных абонентов: открытую аутентификацию (Open Authentication) и аутентификацию с общим ключом (Shared Key Authentication). В аутентификации в беспроводных сетях также широко используются два других механизма, выходящих за рамки стандарта 802.11, а именно назначение идентификатора беспроводной локальной сети (Service Set Identifier - SSID) и аутентификация абонента по его MAC-адресу (MAC Address Authentication).

Принцип аутентификации абонента в IEEE 802.11

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. Процесс аутентификации абонента беспроводной локальной сети IEEE 802.11 состоит из следующих этапов (рис. 9.1):

Абонент (Client) посылает фрейм Probe Request во все радиоканалы.

Каждая точка радиодоступа (Access Point - AP), в зоне радиовидимости которой находится абонент, посылает в ответ фрейм Probe Response.

Абонент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request).

Точка радиодоступа посылает подтверждение аутентификации (Authentication Reply).

В случае успешной аутентификации абонент посылает точке радиодоступа фрейм ассоциации (Association Request).

Точка радиодоступа посылает в ответ фрейм подтверждения ассоциации (Association Response).

Абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.