**Проблемы беспроводных сетей**

**Ver3**

**Mesh-сети**

**Безопасность.**

Развитие беспроводных сетей и удобство их использования актуализирует проблему обеспечения безопасности взаимодействия составляющих элементов. В настоящее время беспроводные сети включают 3G, LTE, а также сети стандарта 802.1x. Для компрометирования проводной сети злоумышленнику необходимо получить доступ к сети изнутри: проникнуть в здание, найти сетевую розетку, подключиться к розетке со своего ноутбука. Сделать это очень трудно без применения методов социальной инженерии. В случае беспроводной сети злоумышленнику достаточно находиться недалеко от здания, чтобы получить возможность доступа к сети. Кроме того, весь трафик от точки доступа до клиента распространяется во всех направлениях в зоне покрытия данной точки доступа.

Для сетей WiFi стандарта 802.11 некоторое время использовался алгоритм шифрования данных WEP. На смену WEP пришел WPA, поддерживающий EAP (расширяемый протокол аутентификации) и шифрование AES. Алгорритм WPA является менее защищенным, чем WPA2, но более широко распространен, например, в сетях WiMAX, а также в сетях с «бесшовным роумингом», для которых необходим сервер с базой зарегистрированных пользователей RADIUS. Сервер аутентификации генерирует уникальный ключ для сеанса связи, TKIP отвечает за увеличение размера ключа, отвечает за передачу ключа пользователю.

WPA = 802.1X + EAP + TKIP + MIC

С 2006 года поддержка WPA2 является обязательным условием для сертификации WiFi-устройств. Протокол WPA2 включает два типа WPA2 Personal и WPA2 Enterprice. Разница между этими двумя типами заключается в том, откуда берутся ключи для шифрования AES: в настройке точки доступа или же на RADIUS-сервере. В отличии от WPA, WPA2 использует AES шифрование, вместо CR4.

Стандартные процедуры обеспечения защиты информации в сетях включают следующие этапы.

Аутентификация и авторизация пользователей. Аутентификация проводится на этапе соединения с точкой доступа, т.е. еще до получения пользователем ip-адреса. После успешной аутентификации пользователю необходимо дождаться авторизации, согласно которой пользователю будут доступны ресурсы.

Для разделения трафика разных классов применяются VLANы. Первоначально они использовались в проводных сетях, но также могут использоваться и в беспроводных. При этом трафик разделяется на трафик локальной сети предприятия, и “гостевой” трафик, порождаемый незарегистрированными устройствами. Это позволяет воспрепятствовать получению доступа к внутренней сети предприятия с неизвестного смартфона, даже при условии подключения зарегистрированного и незарегистрированного устройства к одной точке доступа.

Еще одной задачей является фильтрация трафика с применением фаерволов на основе ip-адресации. Такая фильтрация часто используются для обеспечения защиты доступа для удаленных сотрудников, соединяющихся с внутренними ресурсами компании, например, из дома при помощи программ VPN. Следует заметить, что межсетевые экраны рекомендовано устанавливать непосредственно на источнике пакетов, тем самым достигается значительное снижение объема трафика в сети.

**Проблемы маршрутизации**

Заключение:

В данной статье рассмотрены статические и динамические, одномаршрутные и многомаршрутные, одноуровневые и иерархические типы алгоритмов маршрутизации, так же описаны алгоритмы маршрутизации с маршрутизацией от источника и междоменные и внутридоменные алгоритмы. Кроме того, приведены примеры протоколов для дистанционно-векторной маршрутизации и маршрутизации по состоянию канала.

В данной статье приведены проблемы беспроводных mesh- сетей – безопасность, создающая дополнительные проблемы при организации любых беспроводных сетей, и сама маршрутизация.

5G, Li-fi, Project Loon и беспилотники Facebook, mesh-сети и интернет вещей — все эти тренды ведут к тому, что граница между миром реальным и виртуальным окончательно теряет четкость.

С развитием технологий связано множество острых проблем, и технических, и социальных, и юридических, так что вряд ли будущее будет похоже на цифровую утопию. Но лучшее, что можно сделать, чтобы справиться с этими вызовами — обеспечить как можно большему числу людей доступ к современным технологиям связи, в надежде, что сообща они не только найдут приемлемые решения, но и сделают реальность качественно лучше.