ЗАЩИТА КОМПЬЮТЕРНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

РЕПОЗИТОРИЙ ГГУ ИМЕНИ ФРАНЦИСКА СКОРИНЫ

Контроль границы сети

Граница сети – радиуса охвата радиосети. Такой контроль производится путем ограничения зоны распространения радиосигнала, что позволяет решить 2 задачи: снизить вероятность обнаружения радиосети и уменьшить расстояние, с которого злоумышленник может осуществлять активные или пассивные атаки.

Для ограничения радиуса охвата радиосети могут использоваться:

- аттенюаторы (устройства, предназначенные для снижения уровня сигналов, обеспечивающие фиксированное или регулируемое затухание)
- снижение мощности передатчика встроенными средствами точки доступа
- использование направленных антенн и просто правильная ориентация антенн в пространстве.
- размещения точек доступа в отдалении от границ здания.
- покраска стен помещений с помощью специальной краски, обладающей высоким коэффициентом поглощения в частотном диапазоне, используемом радиосетями
- установка помех в частотном диапазоне радиосетей

Скрытие SSID

В служебных фреймах Beacon и ProbeResponse точка доступа отправляет идентификатор сети и другие служебные данные.

Стандартом предусмотрена и в большинстве точек доступа реализована возможность отключать широковещательную рассылку SSID. Этот режим обычно называется disablessidbroadcast или noguestmode. В результате в поле SSID во фреймах Beacon и ProbeResponse будет указываться пустая строка. Такие сети не будут отображаться в утилитах типа Netstumbler и не будут видны в списке доступных сетей стандартного беспроводного клиента.

Все станции в сети, подключенные к точке доступа, знают SSID и при подключении, когда рассылают ProbeRequest запросы, указывают идентификаторы сетей, имеющиеся в их профилях подключений. Если точка доступа отвечает на такой фрейм, значит, ее SSID совпадает со значением, указанным в запросе, и можно приступать к процедуре подключения.

Однако данный способ не обеспечивает должного уровня защиты, так как злоумышленник, прослушивающий сеть в режиме мониторинга, имеет возможность узнавать идентификатор сети. Существует большое количество утилит, работающих по такому принципу, например, популярный анализатор беспроводных сетей Kismet. Однако, несмотря на свои недостатки, данный механизм защиты безусловно, является полезным для обеспечения защищенности сети.

Аутентификация IEEE 802.11X

При использовании протокола 802.1X станция, физически подключающаяся к сети, не получает доступа к другим узлам до прохождения аутентификации. За реализацию этой функции отвечает активное сетевое оборудование, отключающее станции от сети до получения положительного вердикта об их аутентичности. Устройство, выполняющее подобные функции, называется аутентификатором (Authenticator). Функции аутентификации не выполняются непосредственно на коммутаторе, аутентификатор используется в качестве сервера-посредника между инициатором и третьим компонентом 802.1X, сервером аутентификации (AuthenticationServer). В роли сервера аутентификации может быть использована практически любая реализация сервера RADIUS.

При подключении к сети аутентификатор посылает инициатору по протоколу ExtensibleAuthenticationProtocoloverLAN (EAPOL) запрос на аутентификацию. Если клиент не поддерживает 802.1X, запрос игнорируется, и станция не имеет возможности взаимодействия с сетью. В противном случае клиент инициирует протокол проверки подлинности, в ходе которого происходит взаимная аутентификация сервера RADIUS и подключаемой станции. Аутентификатор преобразует запросы EAPOL в команды протокола RADIUS и обратно. Если клиент успешно прошел аутентификацию и авторизацию, сервер RADIUS дает аутентификатору команду на подключение к сети, после чего станция получает возможность взаимодействия в рамках контролируемого коммутатором или точкой доступа сегмента. Дополнительно сервер RADIUS может генерировать и передавать точке доступа и подключаемой станции ключи шифрования (WEP, PMK для WPA или WPA2).

Аутентификация по MAC — адресам

Большинство точек доступа и беспроводных коммутаторов позволяет указывать черные и белые списки MAC — адресов станций, которым запрещено (или разрешено) подключаться к сети. MAC — адрес — это 48-битный адрес для каждого устройства. Первые 24 бита относятся к производителю и являются общими для всех устройств, сделанных им. Оставшиеся 24 бита являются уникальными для каждого устройства. Обычно каждый сетевой адаптер нумеруется последовательно при помощи этого уникального номера, который является своеобразным идентификатором устройства для всей остальной сети.

Для ограничения доступа с помощью фильтрации MAC – адресов используют 2 метода:

- Точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;
- Точка доступа запрещает доступ станциям, чьи MAC-адреса находятся в “чёрном списке”;

Конфигурирование структуры пакетов

Пройдемся по каждой составляющей в структуре пкаета:

- Преамбула - служит настройкой для сетевой карты (обработка пакетов и их прием)
- идентификатор приемника - идентификатор, который есть у каждого абонента в сети (сетевой адрес).
- идентификатор передатчика - тот же сетевой адрес, но принимающей стороны
- данные для управления обработкой - в этом поле содержатся основные ведения, касающиеся передаваемого пакета:
- размер
- формат
- маршрут
- тип
- номер
- данные - основная информация, ради которой и используются пакеты, т.е. передаваемые данные
- контрольная сумма - специальное число, служащее проверкой целостности пакета
- стоповая комбинация - фиксирует окончание передачи пакета

Криптозащита

Широкое распространение для защиты БС приобрели два алгоритма:

- WEP, основанный на RC4,
- WPA, основанный на AES.

Достоинства алгоритма WEP:

- возможность периодической смены ключа и частой смены вектора инициализации;
- самосинхронизация шифра по каждому сообщению, что снижает вероятность потери пакетов;
- эффективность алгоритма и возможность его реализации как программными, так и аппаратными средствами;
- статус дополнительной возможности, что позволяет пользователю самому решать вопрос об использовании этого алгоритма.

Можно отметить следующие преимущества, относящиеся к аспектам реализации AES алгоритма:

- AES может выполняться быстрее, чем обычный блочный алгоритм шифрования за счет выполнения оптимизация между размером таблицы и скоростью выполнения;
- преобразование раунда допускает параллельное выполнение, что является важным преимуществом для будущих процессоров и специализированной аппаратуры;
- алгоритм шифрования не использует арифметические операции, поэтому тип архитектуры процессора не имеет значения;
- алгоритм шифрования полностью «самоподдерживаемый», то есть он не использует других криптографических компонентов;
- длины блоков от 192 до 256 бит позволяют создавать хэш — функции без коллизий, использующие AES в качестве функции сжатия;
- разработка позволяет специфицировать варианты длины блока и длины ключа в диапазоне от 128 до 256 бит с шагом в 32 бита;

Оптимизация конфигурации беспроводного сегмента сети

- Во многих случаях угрозой является неправильно сконфигурированный беспроводной сегмент сети. В этом случае необходимо улучшение конфигурации. Это может быть изменение конфигурации конфигурации всей сети или отдельных её компонентов

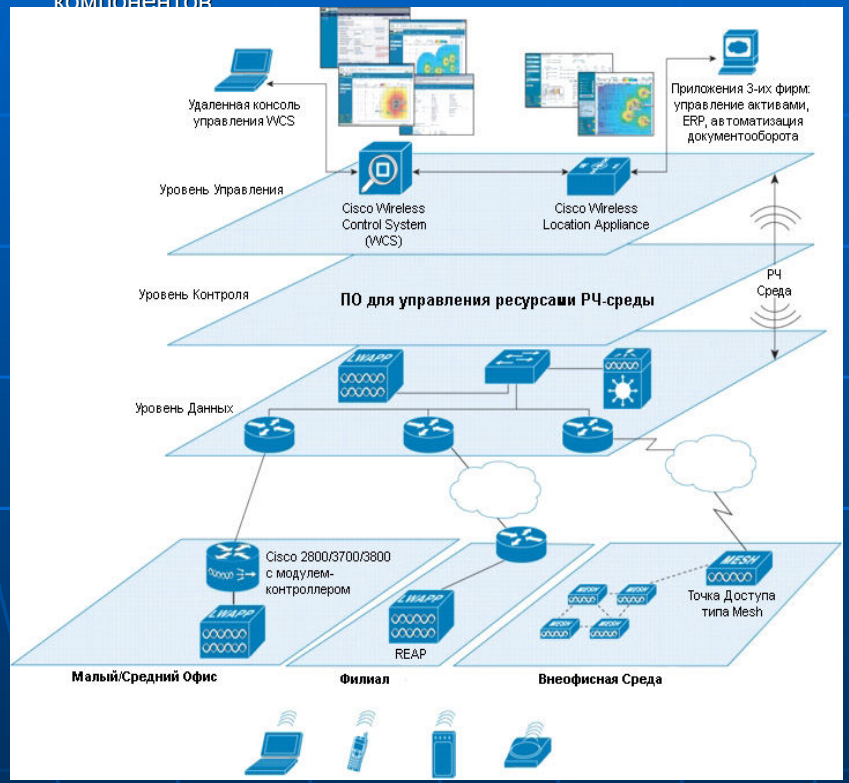

Схема подключения "облегченной" точки доступа

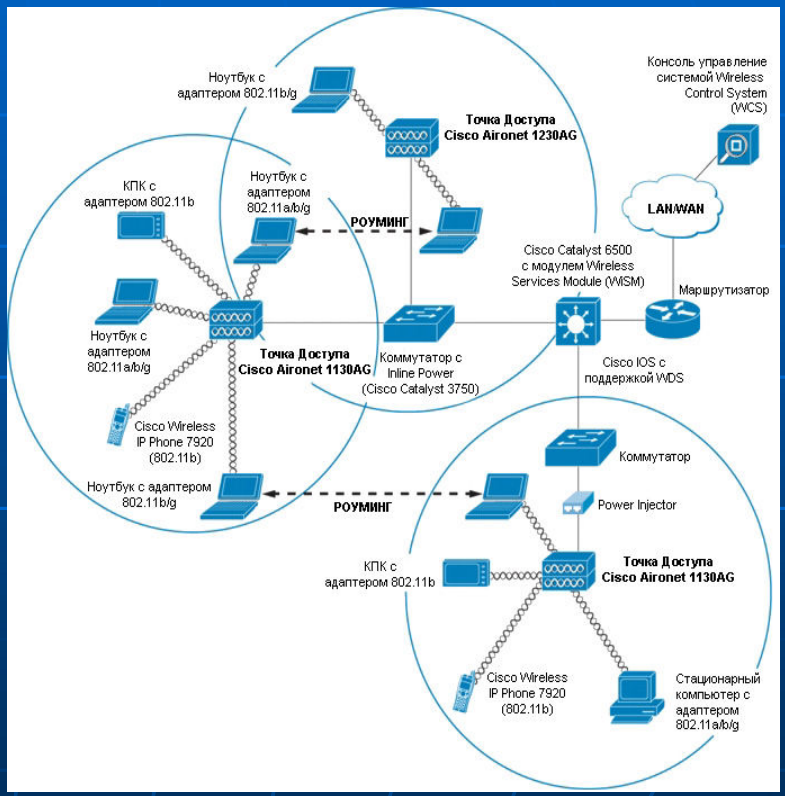

Схема подключения автономной точки доступа