WEP на примере конфигурации автономной точки доступа

Содержание

Введение

Этот документ описывает, как использовать и настроить Протокол WEP на Автономной точке доступа Cisco (AP).

Предварительные условия

Требования

Этот документ предполагает, что можно сделать административное соединение к устройствам WLAN, и что устройства обычно функционируют в нешифрованной среде. Для настройки стандартного 40-разрядного WEP у вас должно быть два или больше радиоустройства, которые связываются друг с другом.

Используемые компоненты

Сведения в этом документе основываются на AP 1140 года, который выполняет Cisco IOS® Release15.2JB.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

потенциальное воздействие всех команд до их использования.

Общие сведения

WEP является алгоритмом шифрования, встроенным в 802.11 (Wi-Fi) стандарт. WEP использует поточный шифр RC4 для конфиденциальности и Cyclic Redundancy Checks 32 (CRC-32) контрольная сумма для целостности .

Стандартный 64-разрядный WEP использует ключ на 40 битов (также известный как WEP 40), который связан с 24-разрядным Вектором инициализации (IV) для формирования ключа RC4. 64-разрядный Ключ WEP обычно вводится как строка 10 шестнадцатеричных (базируйтесь 16), символы (нуль до девять и A-F). Каждый символ представляет четыре бита, и десять цифр четырех битов, каждый равняется 40 битам; если вы добавляете 24-разрядный IV, он производит завершенный 64-разрядный Ключ WEP.

128-разрядный Ключ WEP обычно вводится как строка 26 шестнадцатеричных символов. Двадцать шесть цифр четырех битов каждый equals104 биты; если вы добавляете 24-разрядный IV, он производит завершенный 128-разрядный Ключ WEP. Большинство устройств позволяет пользователю вводить ключ как 13 ASCII - символов.

Методы аутентификации

Два метода проверки подлинности могут использоваться с WEP: Аутентификация открытой системы и Проверка подлинности с общим ключом.

С Аутентификацией открытой системы клиент WLAN не должен предоставлять учетные данные AP для аутентификации. Любой клиент может аутентифицироваться с AP, и затем попытаться связаться. В действительности никакая аутентификация не происходит. Впоследствии, Ключи WEP могут использоваться для шифрования фреймов данных. На этом этапе у клиента должны быть корректные ключи.

С Проверкой подлинности с общим ключом Ключ WEP используется для аутентификации в квитировании ответа на запрос с четырьмя шагами:

1. Клиент передает запрос аутентификации к AP.
2. AP отвечает с проблемой открытого текста.
3. Клиент шифрует текст запроса с настроенным Ключом WEP и отвечает другим запросом аутентификации.
4. AP дешифрует ответ. Если ответ совпадает с текстом запроса, AP передает положительный ответ.

После аутентификации и ассоциации, предварительный общий Ключ WEP также используется для шифрования фреймов данных с RC4.

На первый взгляд могло бы казаться, как будто Проверка подлинности с общим ключом более безопасна, чем Аутентификация открытой системы, начиная с последних предложений никакая реальная аутентификация. Однако реверс истинен. Возможно получить keystream, используемый для квитирования при получении кадров с вопросом в Проверке подлинности с общим ключом. Следовательно, желательно использовать Аутентификацию открытой системы для аутентификации WEP, а не Проверку подлинности с

общим ключом.

Протокол TKIP был создан для решения этих проблем WEP. Подобный WEP, TKIP использует шифрование RC4. Однако TKIP улучшает WEP с добавлением мер, таких как попакетное хеширование ключей, Message Integrity Check (MIC) и Ротация (широковещательных) ключей для адресации к известным уязвимостям WEP. TKIP использует поточный шифр RC4 с 128-разрядными ключами для шифрования и 64-разрядными ключами для аутентификации.

Настройка

Этот раздел предоставляет GUI и конфигурации интерфейса командой строки для WEP.

Конфигурация графического интерфейса пользователя (GUI)

Выполните эти шаги для настройки WEP с GUI.

1. Соединитесь с AP через GUI.
2. Из Меню системы безопасности на левой части окна выберите **Encryption Manager** для радиоинтерфейса, к которому вы хотите настроить свои статические ключи WEP.
3. Под Режимами шифрования нажмите **WEP Encryption** и выберите **Mandatory** от раскрывающегося меню для клиента.

   Режимы шифрования, используемые Станцией:
   По умолчанию (Никакое Шифрование) - требования клиента для передачи с AP без любого шифрования данных. Эта установка не рекомендуется.**Дополнительный** - Позволяет клиентам связываться с AP или с или без шифрования данных. Как правило, вы используете эту опцию, когда у вас есть устройства клиента, которые не могут сделать WEP - подключение, такой как клиенты не-Cisco в 128-разрядной среде WEP.**Обязательный (Полное шифрование)** - требования клиента для использования шифрования данных, когда они связываются с AP. Клиентам, которые не используют шифрование данных, не разрешают связаться. Если вы хотите увеличить безопасность своего WLAN, эта опция рекомендуется.
4. Под Ключами шифрования установите переключатель **Transmit Key** и введите 10-разрядный шестнадцатеричный ключ. Гарантируйте, что Размер ключа установлен в **40 битов**.

   Введите 10 шестнадцатеричных цифр для 40-разрядных Ключей WEP или 26 шестнадцатеричных цифр для 128-разрядных Ключей WEP. Ключи могут быть любой комбинацией этих цифр:
   От 0 до 9к fK F
5. Нажмите **Apply-All** для применения конфигурации по обоим из радио.
6. Создайте идентификаторы наборов сервисов (SSID) с **Открытой аутентификацией** и нажмите **Apply** для включения его на обоих радио.

7. Перейдите к сети и включите радио для **2.4 ГГц** и **5 ГГц** для получения их выполнение.

Конфигурация интерфейса командой строки CLI

Используйте этот раздел для настройки WEP с CLI.

```
ap#show run
Building configuration...

Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
 dot11 ssid wep-config
 authentication open
 guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
```

```
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

Проверка

Введите эту команду, чтобы подтвердить, что ваша конфигурация работает должным образом:

```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address   IP address     Device       Name          Parent        State
1cb0.94a2.f64c 10.106.127.251 unknown      -             self          Assoc
```

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Эти **команды отладки** полезны для устранения проблем конфигурации:

- **события debug dot11** - Включают отладку для всех событий dot1x.
- **пакеты debug dot11** - Включают отладку для всех пакетов dot1x.

Вот пример журнала, который отображается, когда клиент успешно связывается к WLAN:

```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address   IP address     Device       Name          Parent        State
1cb0.94a2.f64c 10.106.127.251 unknown      -             self          Assoc
```

Когда клиент вводит неправильный ключ, эта ошибка показы:

```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address   IP address     Device       Name          Parent        State
1cb0.94a2.f64c 10.106.127.251 unknown      -             self          Assoc
```