Обзор конфигурации WPA

Содержание

Введение

Этот документ содержит образец настройки для защищенного доступа Wi-Fi (WPA), внутреннего стандарта безопасности, используемого членами альянса Wi-Fi.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Основательные знания беспроводных сетей и вопросов их безопасности
- Знание методов безопасности Протокола EAP

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco точки доступа IOS® Software-based (AP)

- Программное обеспечение Cisco IOS версии 12.2 (15) JA или позже**Примечание:** Предпочтительно, используйте последний Cisco IOS Software Release, даже при том, что WPA поддерживается в программном обеспечении Cisco IOS версии 12.2(11)JA и позже. Для получения последней версии ПО Cisco IOS перейдите на страницу Downloads (только для зарегистрированных пользователей) .
- Совместимый WPA Network Interface Cards (NIC) и его совместимое WPA клиентское программное обеспечение

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.

Теоретические сведения

Средства безопасности в беспроводной сети, такой как WEP, достаточно слабые. Группа разработчиков Wi-Fi Alliance (или WECA) представила новый внутренний стандарт безопасности нового поколения для беспроводных сетей. Этот стандарт предусматривает дополнительную защиту до официального принятия стандарта 802.11i организацией IEEE.

Данная схема создает на текущем EAP/802.1x аутентификацию и динамическое управление ключами и добавляет более стойкое шифрование. После установления соединения EAP/802.1x клиентсткого устройства и сервера аутентификации управление ключами WPA согласовывается между точкой доступа и клиентским устройством, совместимым с WPA.

Точки доступа Cisco также предлагают гибридную настройку, в которой оба традиционных EAP клиента на основе WEP (с сохранением профиля или без управления ключами) работают в соединении с клиентами WPA. Эта настройка часто называется режимом миграции. Он предусматривает поэтапный подход к миграции на WPA. Режим миграции в этом документе не рассматривается. В этом документе описана структура сети, защищенной WPA.

Помимо безопасности на корпоративном уровне WPA также обеспечивает версию предварительного ключа (WPA-PSK), предназначенного для использования в небольших офисах, домашних офисах (SOHO) или беспроводных внутренних сетях. Клиентская служебная программа Cisco (ACU) не поддерживает WPA-PSK. Программа нулевой беспроводной настройки от Microsoft Windows, так же как и приведенные ниже программы, поддерживают WPA-PSK для большинства беспроводных карт:

- AEGIS Client from Meetinghouse Communications**Примечание:** См. EOS и объявление EOL для Meetinghouse линейка продуктов AEGIS.
- Odyssey client from Funk Software**Примечание:** См. центр службы поддержки пользователей сетей Juniper.
- Служебные программы клиента Original Equipment Manufacturer (OEM) от некоторых изготовителей

Можно настроить WPA-PSK когда:

- Вы выбираете режим шифрования как шифрование TKIP на вкладке Encryption Manager.
- Вы определяете тип аутентификации, использование управления ключами и предварительный ключ на вкладке GUI Service Set Identifier (SSID) Manager.
- Настройка на вкладке "Диспетчер сервера" не требуется.

Для включения WPA-PSK через интерфейс командной строки (CLI) введите следующие команды. Начните с режима настройки:

```
AP(config)#interface dot11Radio 0 AP(config-if)#encryption mode ciphers tkip AP(config-if)#ssid ssid_name AP(config-if-ssid)#authentication open AP(config-if-ssid)#authentication key-management wpa AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

Примечание: Этот раздел предоставляет только конфигурацию, которая относится к WPA-PSK. Приведенная здесь настройка предназначена только для ознакомления и изучения работы WPA-PSK. Основное внимание в документе уделено настройке WPA.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

WPA основано на текущих методах EAP/802.1x. В этом документе предполагается наличие настройки LEAP, EAP или PEAP, которая работает перед добавлением настройки для привлечения WPA.

В этом разделе представлены сведения по настройке функций, описанных в данном документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Сетевой расширенный протокол аутентификации (EAP) или открытая аутентификация с применением EAP

При использовании метода аутентификации на основе EAP/802.1x возникает вопрос о различиях между сетевым EAP и открытой аутентификацией с применением EAP. Это относится к значениям в поле Authentication Algorithm в заголовках пакетов управления и связывания. Большинство производителей беспроводных клиентских устройств устанавливают значение этого поля 0 (открытая аутентификация), а затем сообщают о желании провести аутентификацию EAP позднее, во время процесса ассоциации. В продуктах Cisco значение задается по-другому, начиная со связывания с флагом сетевого протокола EAP.

Используйте приведенный ниже метод аутентификации, если ваша сеть имеет следующих клиентов:

- Клиенты Cisco - используют сетевой расширенный протокол аутентификации (EAP).
- Клиентами стороннего производителя (включая продукты, совместимые с CCX [разрешения, совместимые с Cisco]) должна использоваться открытая аутентификация с EAP.
- Использующим сочетание клиентских устройств Cisco и сторонних производителей необходимо выбрать и сетевой EAP и открытую аутентификацию с EAP.

Конфигурация интерфейса командой строки CLI

Эти конфигурации используются в данном документе:

- Конфигурация LEAP, которая существует и работает
- Программное обеспечение Cisco IOS версии 12.2 (15) JA для AP на основе ПО Cisco IOS

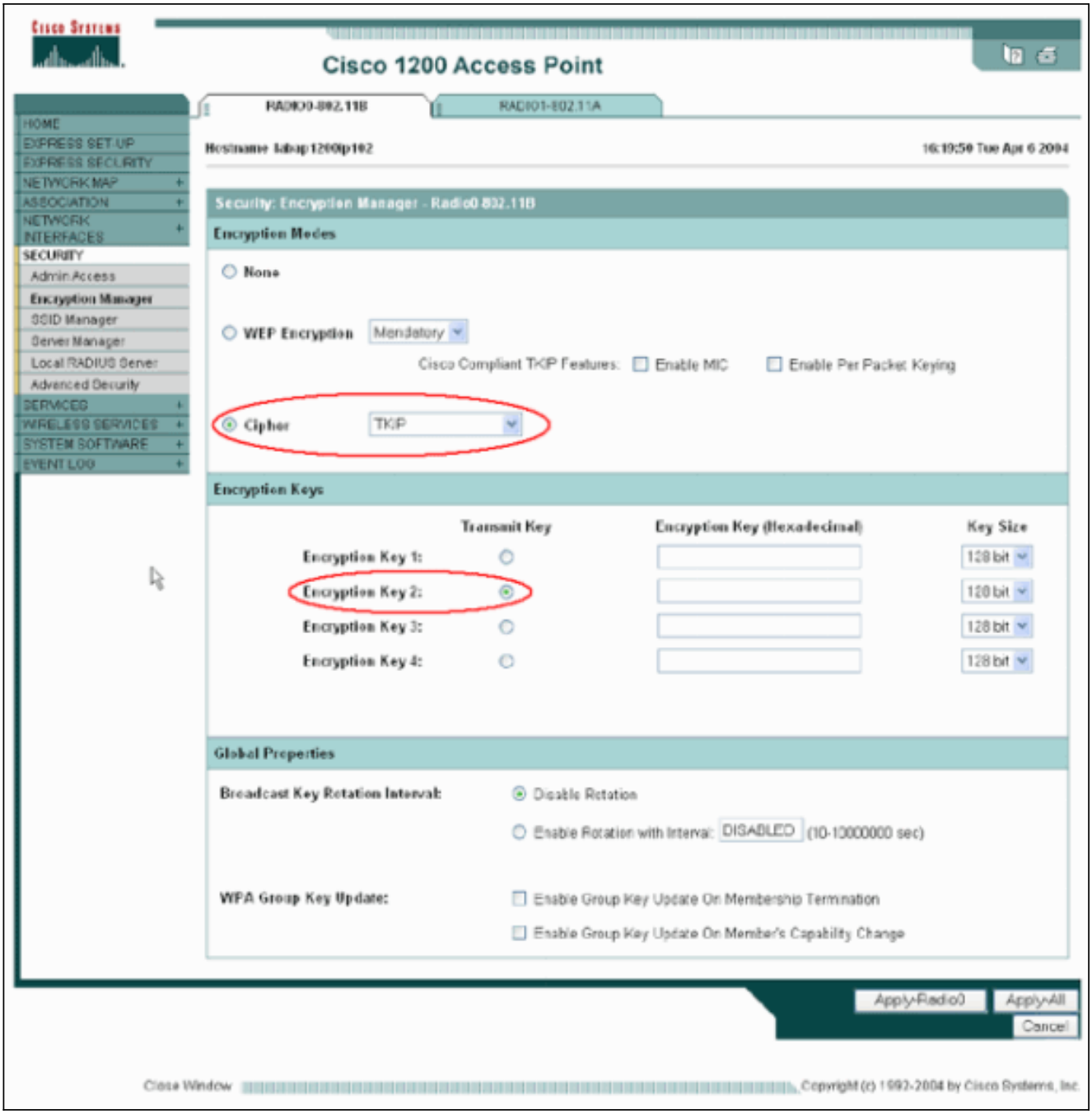
AP

```
ap1#show running-config Building configuration... . . .
aaa new-model ! aaa group server radius rad_eap server
192.168.2.100 auth-port 1645 acct-port 1646 . . aaa
authentication login eap_methods group rad_eap . . . !
bridge irb ! interface Dot11Radio0 no ip address no ip
route-cache ! encryption mode ciphers tkip !--- This
defines the cipher method that WPA uses. The TKIP !---
method is the most secure, with use of the Wi-Fi-defined
version of TKIP. ! ssid WPAlabap1200 authentication open
eap eap_methods !--- This defines the method for the
underlying EAP when third-party clients !--- are in use.
authentication network-eap eap_methods !--- This defines
the method for the underlying EAP when Cisco clients are
in use. authentication key-management wpa !--- This
engages WPA key management. ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 192.168.2.108 255.255.255.0
!--- This is the address of this unit. no ip route-cache
! ip default-gateway 192.168.2.1 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end ! end
```

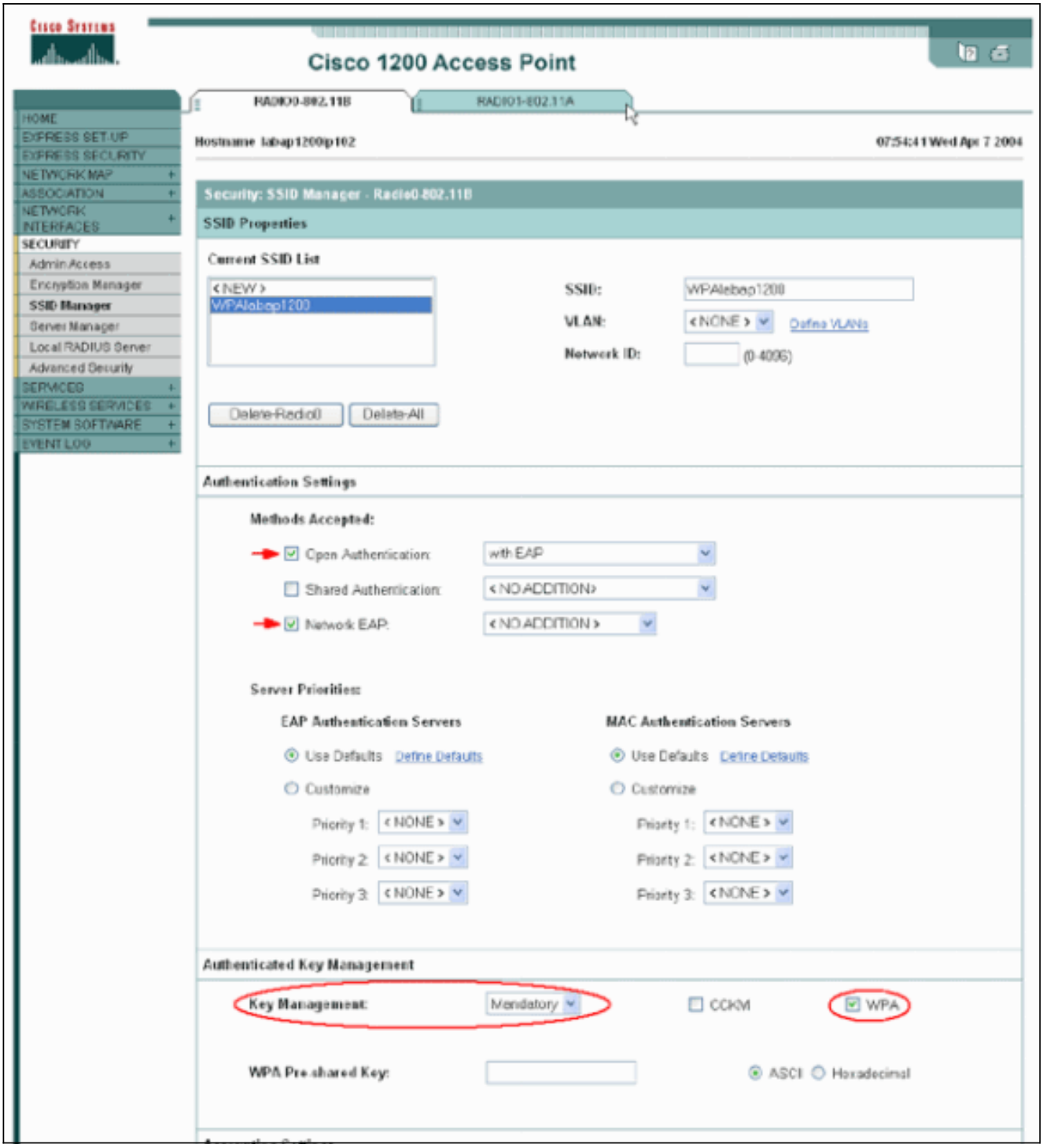
Конфигурация графического интерфейса пользователя (GUI)

Выполните эти шаги для настройки AP для WPA:

1. Выполните следующие шаги для настройки диспетчера шифрования:Включите шифр для TKIP.Очистите значение в ключе шифрования 1.Установите ключ шифровнаия 2 в качестве ключа передачи.***Щелкните Apply-Radio#.***



2. Выполните следующие шаги для настройки диспетчера SSID:Выберите необходимый SSID из текущего списка SSID.Выберите подходящий метод аутентификации.Выбор осуществляется на основе типа используемой клиентской карты. Обратитесь к разделу Сетевой расширенный протокол аутентификации (EAP) или открытая аутентификация с применением EAP этого документа для получения дополнительной информации. Если EAP работал и до добавления WPA, то, возможно, не потребуется дополнительных изменений.Выполните следующие шаги для включения управления ключами:**Выберите Mandatory из выпадающего меню Key Management.**Установите флажок WPA.***Щелкните Apply-Radio#.***

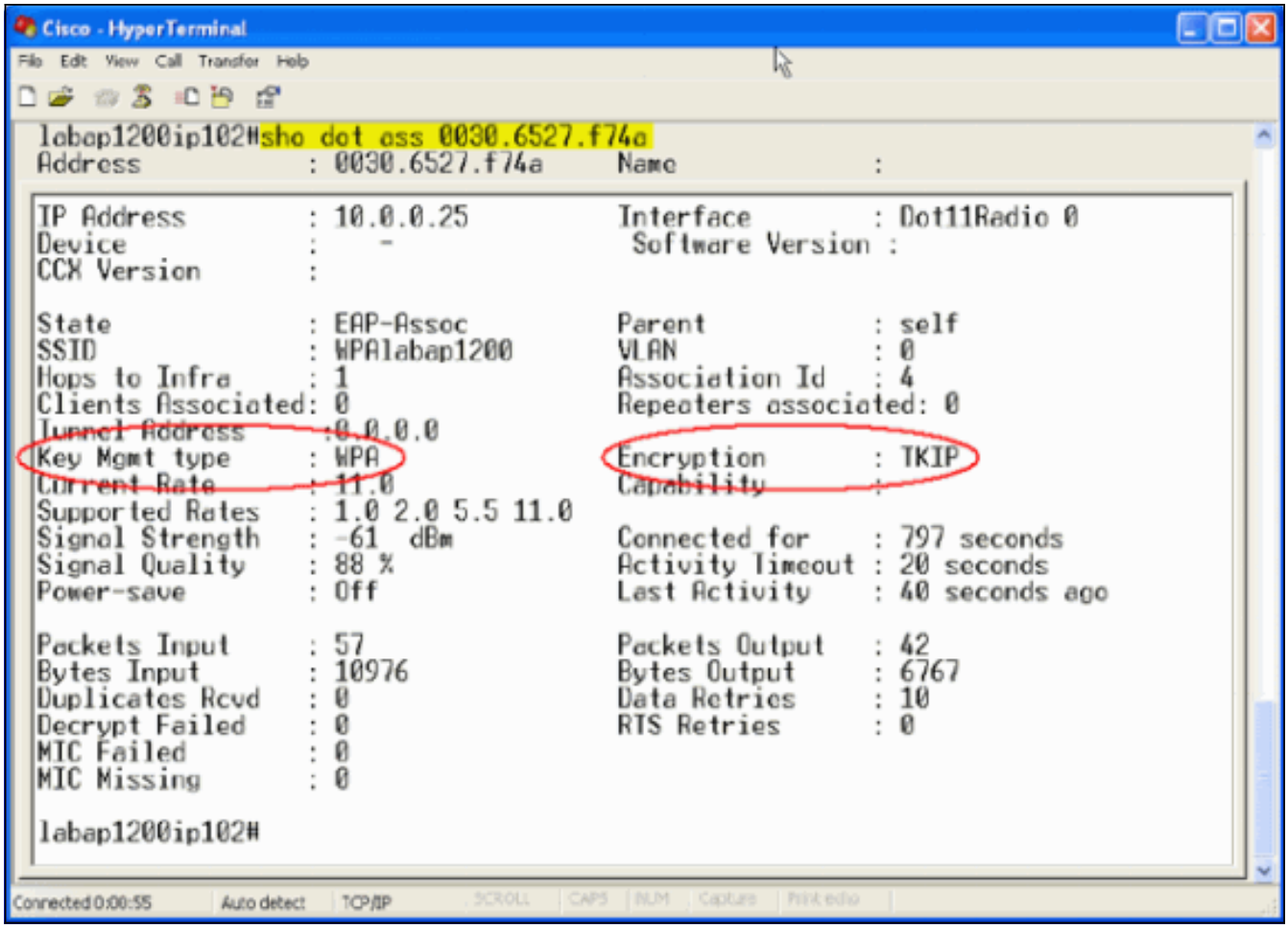


Проверка

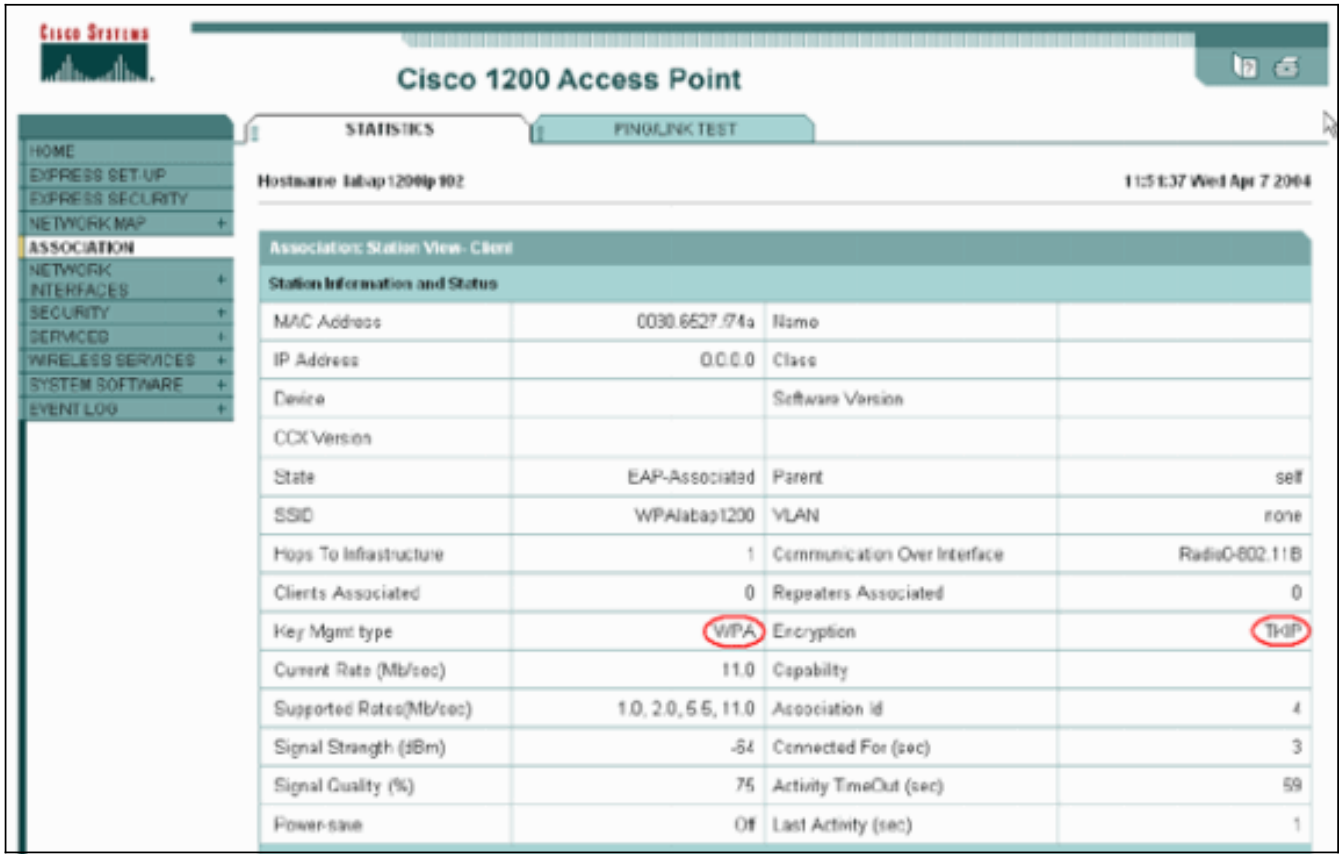
Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **покажите** *mac_address* **ассоциации dot11** — Эта команда отображает информацию о специально определенном связанном клиенте. **Убедитесь, что при согласовании клиент использует для управления ключами WPA, а для шифрования - TKIP.**



- **Значение таблицы связываний для каждого клиента должно также отображать управление ключами как WPA и шифрование как TKIP.** В таблице связываний щелкните MAC-адрес клиента, чтобы просмотреть сведения о связывании для этого клиента.



Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Процедура устранения неполадок

Эти сведения относятся к данной конфигурации. Выполните следующие шаги для устранения неполадки в вашей настройке:

1. Если эта настройка LEAP, EAP или PEAP недостаточно протестирована перед внедрением WPA, необходимо выполнить следующие шаги:Временно отключите режим шифрования WPA.Отмена запрета на соответствующий протокол EAP.Убедитесь, что система аутентификации работает.
2. Проверьте, что настройка клиента соответствует настройке точки доступа.Например, если точка доступа настроена для WPA и TKIP, подтвердите, что настройки соответствуют этим настройкам на клиенте.

Команды устранения неполадок

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

Управление ключами WPA предусматривает четырехэтапное установление связи после успешного завершения аутентификации EAP. Эти четыре сообщения можно увидеть при отладке. Если EAP не подтверждает подлинность клиента или вы не видите этих сообщений, выполните следующие шаги:

1. Временно отключите WPA.
2. Отмена запрета на соответствующий протокол EAP.
3. Убедитесь, что система аутентификации работает.

В списке приведены отладки:

- **менеджер debug dot11 aaa вводит** — Эта отладка показывает квитирование, которое происходит между AP и клиентом WPA, поскольку попарный переходный ключ (PTK) и переходный ключ группы (GTK) выполняют согласование. Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA.Если выходные данные no debug появляются, проверяют эти элементы:**Монитор терминала term mon включен (при использовании сессии Telnet).**Отладки включены.Клиент правильно настроен на WPA.Если отладка показывает, что PTK и/или квитирования GTK созданы, но не проверены, проверьте программное обеспечение инициатора запроса WPA для корректной конфигурации и актуальной версии.
- **конечный автомат средства проверки подлинности debug dot11 aaa** — Эта отладка показывает различные состояния согласований, что клиент проходит, поскольку это связывается и аутентифицируется. Названия состояний отображают эти состояния. Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA. Obsoletes отладки **команда debug dot11 aaa dot1x state-machine** в программном обеспечении Cisco IOS версии 12.2 (15) JA и позже.
- **debug dot11 aaa dot1x state-machine** — Эта отладка показывает различные состояния

согласований, что клиент проходит, поскольку она связывается и аутентифицируется. Названия состояний отображают эти состояния. В Cisco IOS Software Release, которые являются ранее, чем программное обеспечение Cisco IOS версии 12.2 (15) JA, эта отладка также показывает согласование управления ключами WPA.

- **команда debug dot11 aaa authenticator process вЂ. Эта отладка наиболее полезна при диагностике проблем согласованной связи.** Эти подробные сведения показывают, что отправляет каждый участник согласования и каков ответ другого участника. **Эту команду отладки можно также использовать вместе с командой debug radius authentication .** Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA. Obsoletes отладки **команда debug dot11 aaa dot1x process** в программном обеспечении Cisco IOS версии 12.2 (15) JA и позже.
- **debug dot11 aaa dot1x process – помогает выявлять проблемы, связанные с согласованием.** Эти подробные сведения показывают, что отправляет каждый участник согласования и каков ответ другого участника. **Эту команду отладки можно также использовать вместе с командой debug radius authentication .** В ПО Cisco IOS выпуска ранее 12.2(15)JA эта отладка показывает согласование управления ключами WPA.

Дополнительные сведения

- Настройка пакетов Cipher Suites и WEP
- Настройка типов аутентификации
- WPA2 - защищенный доступ по протоколу Wi-Fi 2
- Защищенный доступ по протоколу Wi-Fi 2 (WPA 2) конфигурация
- Cisco Systems – техническая поддержка и документация