Обзор настройки WPA

Необходимо иметь действительную учетную запись Cisco.com для загрузки драйверов, микропрограмм и утилит Cisco Aironet с Downloads - Wireless (только для зарегистрированных пользователей) . Если у вас нет учетной записи на Cisco.com, зарегистрируйтесь бесплатно на Cisco.com Registration .

Содержание

Общие сведения

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

Предварительные условия

Требования

Перед использованием этой настройки убедитесь в выполнении следующих предварительных условий:

- Глубокие знания методов обеспечения безопасности расширенного протокола аутентификации (EAP).
- Знания методов обеспечения безопасности расширенного протокола аутентификации (EAP).

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к следующим версиям программного и аппаратного обеспечения:

- Точки доступа (AP) на основе ПО Cisco IOS®
- ПО Cisco IOS выпуск 12.2(15)JA и выше

Примечание: Наиболее предпочтительно использовать последнюю версию ПО Cisco IOS, даже если WPA поддерживается ПО Cisco IOS выпуска 12.2(11)JA и выше. Для получения последней версии ПО Cisco IOS перейдите на страницу Downloads (только для зарегистрированных пользователей) .

- Совместимая с WPA сетевая интерфейсная плата (NIC) и ее совместимое с WPA клиентское ПО

Данные для документа были получены в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с пустой (стандартной) настройкой. В рабочей сети необходимо изучить потенциальное воздействие всех команд.

Теоретические основы

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: Обратитесь к разделу Meetinghouse Solutions .

- Odyssey client from Funk Software

  Примечание: Обратитесь к разделу Служба поддержки пользователей Juniper Networks .

- Клиентские программы производителей оригинального оборудования (OEM) от некоторых производителей

Вы можете 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 Service Set Identifier (SSID) Manager.
- Настройка на вкладке Server Manager 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: В этом разделе описана только настройка, относящаяся к WPA-PSK. Приведенная здесь настройка предназначена только для ознакомления и изучения работы WPA-PSK. Основное внимание в документе уделено настройке WPA.

Условные обозначения

Обратитесь к разделу Технические советы Cisco. Условные обозначения для получения дополнительных сведений об условных обозначениях в документах.

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 средство поиска команд Command Lookup Tool (только для зарегистрированных пользователей) для получения дополнительной информации о командах, упомянутых 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)
- Клиенты стороннего производителя (в том числе совместимые продукты CCX) – используют открытую аутентификацию с EAP.
- Комбинация клиентов Cisco и посторонних клиентов - используют оба метода аутентификации Network-EAP и открытую аутентификацию с EAP.

Настройка CLI

В данном документе используются следующие настройки:

- Существующая и работающая настройка LEAP
- ПО Cisco IOS выпуск 12.2(15)JA для точек доступа на основе ПО Cisco IOS

AP
ap1#**show running-config** Building configuration... . . . aaa new-model !

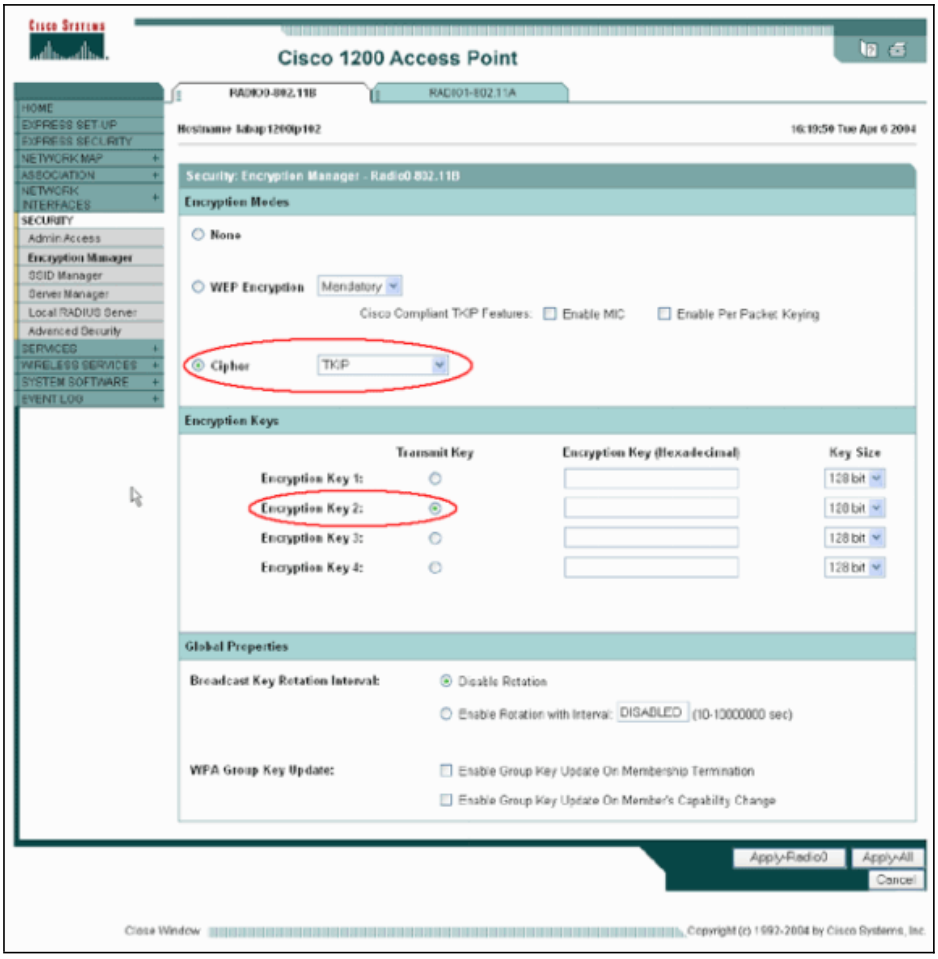
```
aaa group server radius rad_eap
server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip

!--- Здесь описан метод шифрования, используемый в WPA. TKIP - это
!--- наиболее безопасный метод, который использует версию TKIP на основе Wi-Fi.


!
ssid WPAlabap1200
   authentication open eap eap_methods


!--- Здесь определяется метод для основного EAP у сторонних
!--- клиентов.

   authentication network-eap eap_methods


!--- Здесь определяется метод для основного EAP у клиентов Cisco.

   authentication key-management wpa

!--- Это вызывает управление ключами WPA.

!
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

!--- Это адрес модуля.

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/help/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

!--- Здесь определяется местонахождение сервера RADIUS и ключ между точкой доступа и сервером.

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
```

Настройка GUI

Выполните следующие шаги для настройки точки доступа для WPA:

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

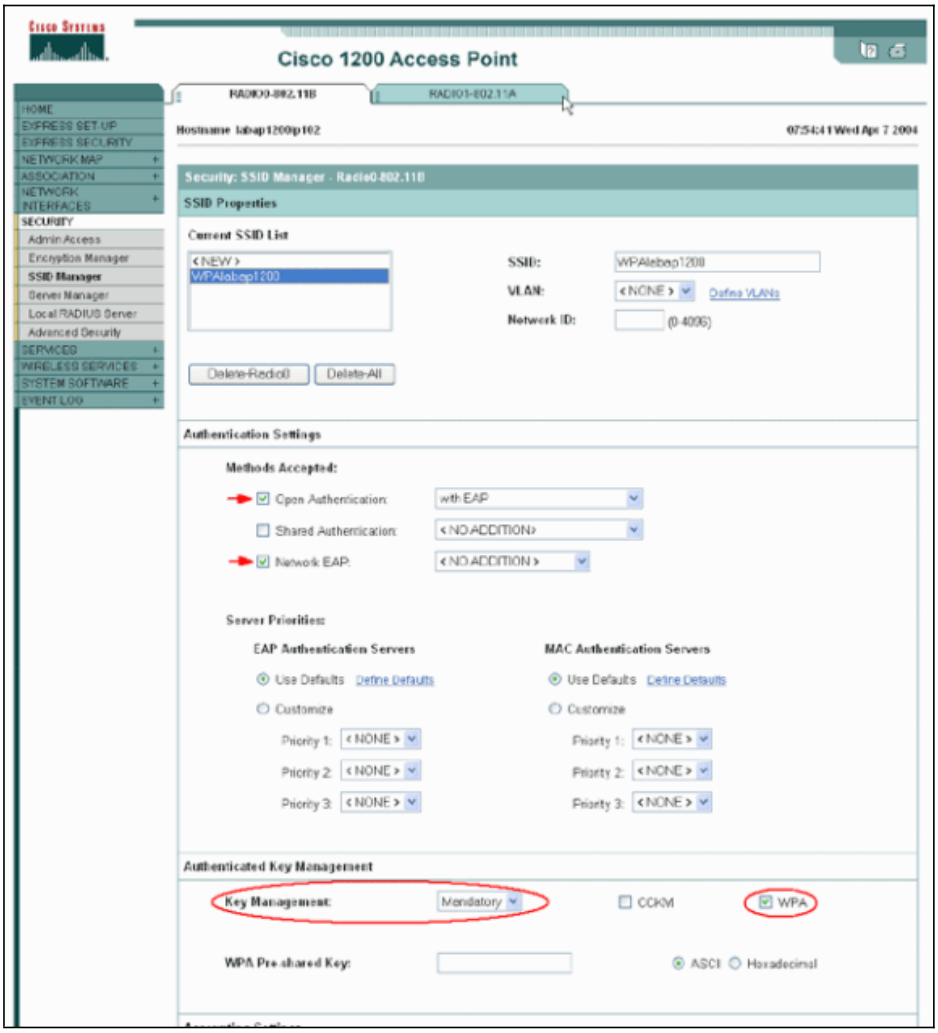


2. Выполните следующие шаги для настройки диспетчера SSID:
    1. Выберите необходимый SSID из текущего списка SSID.
    2. Выберите подходящий метод аутентификации.

        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.
    3. Выполните следующие шаги для включения управления ключами:

1. Выберите **Mandatory** из выпадающего меню Key Management.
2. Установите флажок WPA.

4. Щелкните **Apply-Radio#**.

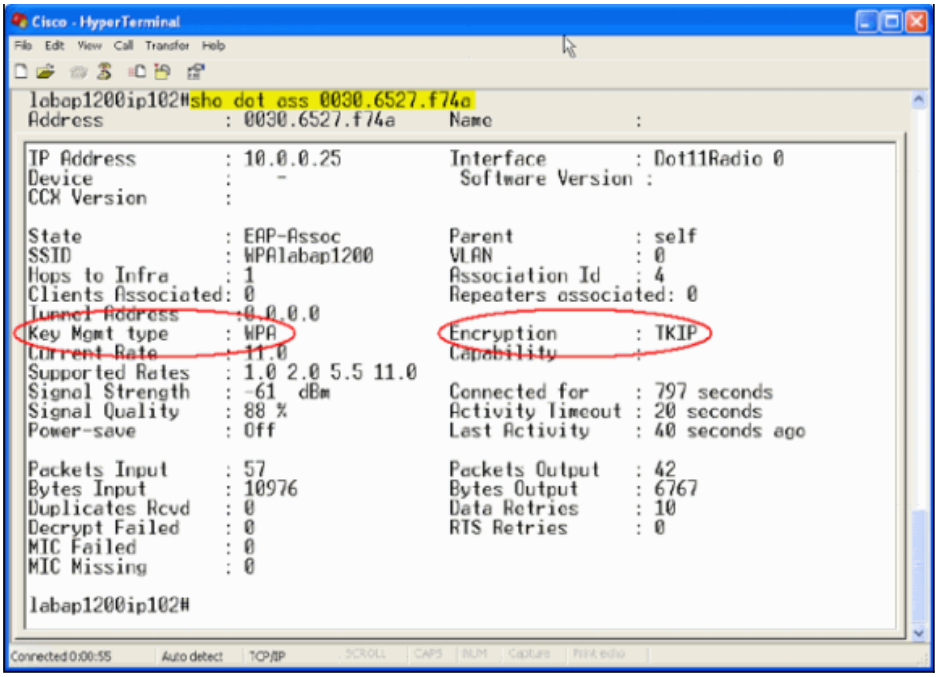


Проверка

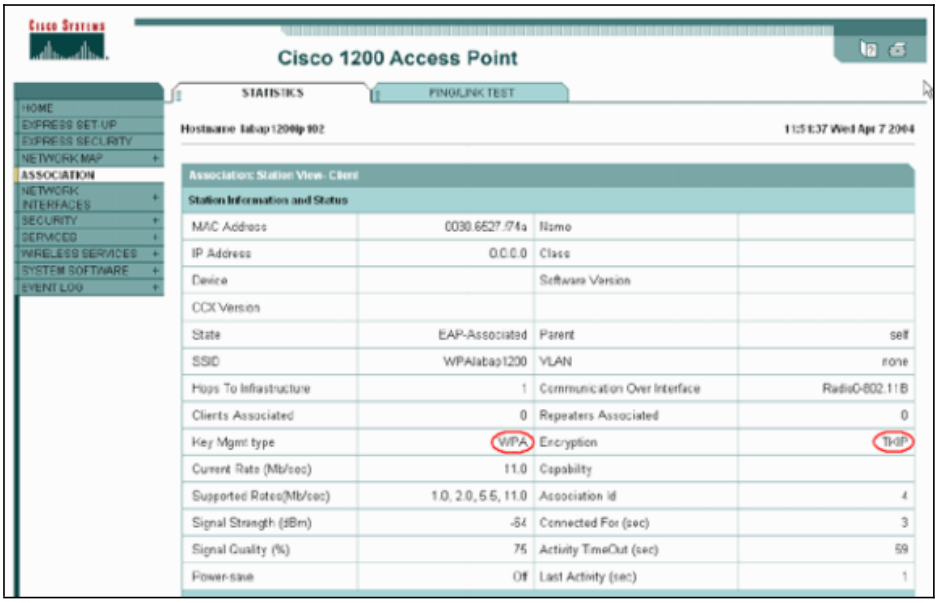
Используйте информацию в том разделе для определения правильности работы вашей настройки.

Интерпретатор выходных данных Output Interpreter Tool (только для зарегистрированных пользователей) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра анализа выходных данных команды **show** .

- **show dot11 association *mac_address***—эта команда выводит информацию о связанном и особым образом идентифицированном 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 данном разделе описывается процесс устранения неполадок настройки.

Процедура устранения неполадок

Эти сведения относятся к данной настройке. 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:
    1. Временно отключите режим шифрования WPA:
    2. Активируйте снова соответствующий EAP.
    3. 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: Обратитесь к разделу Важные сведения о командах отладки перед использованием команд **debug** .

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. Активируйте снова соответствующий EAP.
3. Убедитесь, что система аутентификации работает.

В списке приведены отладки:

- **debug dot11 aaa manager keys**—с помощью данной команды отладки отображаются сведения об обмене с квитированием между точкой доступа и клиентом WPA в процессе согласования PTK и GTK. Эта отладка была представлена в ПО Cisco IOS выпуск 12.2(15)JA.

debug dot11 aaa manager keys
labap1200ip102# **Apr 7 16:29:57.908: dot11_dot1x_build_ptk_handshake: building PTK msg 1 for 0030.6527.f74a** **Apr 7 16:29:590,190: dot11_dot1x_verify_ptk_handshake: verifying PTK msg 2 from 0030.6527.f74a** Apr 7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning: Invalid key info (exp=0x381, act=0x109 Apr 7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning: Invalid key len (exp=0x20, act=0x0) **Apr 7 16:29:590,192: dot11_dot1x_build_ptk_handshake: building PTK msg 3 for 0030.6527.f74a** **Apr 7 16:29:59.783: dot11_dot1x_verify_ptk_handshake: verifying PTK msg 4 from 0030.6527.f74a** Apr 7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning: Invalid key info (exp=0x381, act=0x109 Apr 7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning: Invalid key len (exp=0x20, act=0x0) **Apr 7 16:29:59.788: dot11_dot1x_build_gtk_handshake: building GTK msg 1 for 0030.6527.f74a** Apr 7 16:29:59.788: dot11_dot1x_build_gtk_handshake: dot11_dot1x_get_multicast_key len 32 index 1 Apr 7 16:29:59.788: dot11_dot1x_hex_dump: GTK: 27 CA 88 7D 03 D9 C4 61 FD 4B BE 71 EC F7 43 B5 82 93 57 83 **Apr 7 16:30:01.633: dot11_dot1x_verify_gtk_handshake: verifying GTK msg 2 from 0030.6527.f74a** Apr 7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning: Invalid key info (exp=0x391, act=0x301 Apr 7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning: Invalid key len (exp=0x20, act=0x0) **Apr 7 16:30:01.633: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 0030.6527.f74a Associated KEY_MGMT[WPA]** labap1200ip102#

   Если выходные данные отладки не появляются, проверьте следующие параметры:

   - Монитор терминала **term mon** включен (при использовании сессии Telnet).

- Отладки включены.
- Клиент правильно настроен на WPA.

Если отладка показывает, что связь PTK и/или GTK настроена, но не проверена, проверьте правильность настройки и версию поставляемого с WPA ПО.

- **debug dot11 aaa authenticator state-machine**—эта отладка показывает различные состояния согласования клиента, возникающие во время процесса соединения и аутентификации. На состояние указывает его название. Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA. Отладка опускает команду **debug dot11 aaa dot1x state-machine** в ПО Cisco IOS выпуска 12.2(15)JA и выше.
- **debug dot11 aaa dot1x state-machine**—эта отладка показывает различные состояния согласования клиента во время процесса соединения и аутентификации. Названия состояний отображают эти состояния. В ПО Cisco IOS выпуска ранее 12.2(15)JA эта отладка также показывает согласование управления ключами WPA.
- **debug dot11 aaa authenticator process**—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. Эта отладка опускает команду **debug dot11 aaa dot1x process** в ПО Cisco IOS выпуска 12.2(15)JA и выше.
- **debug dot11 aaa dot1x process**—эта отладка 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**. В ПО Cisco IOS выпуска ранее 12.2(15)JA эта отладка показывает согласование управления ключами WPA.

Дополнительная информация

- **Настройка пакетов Cipher Suites и WEP**
- **Настройка типов аутентификации**
- **Веб-сайт по безопасности защищенного доступа Wi-Fi (WPA)**
- **WPA2 - защищенный доступ Wi-Fi 2**
- **Защищенный доступ Wi-Fi, WPA2 и IEEE 802.11i**
- **Настройка защищенного доступа Wi-Fi 2 (WPA 2)**
- **Техническая поддержка и документация - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92183/WPAOverview.shtml