Пример настройки гостевой беспроводной локальной сети (WLAN) и внутренней беспроводной локальной сети при использовании контроллеров беспроводных локальных сетей (WLC)

Содержание

Введение

В данном документе представлен пример конфигурации для гостевой беспроводной локальной сети (WLAN) и защищенной внутренней WLAN, которая использует контроллеры WLAN (WLC) и упрощенные точки доступа (LAP). В примере конфигурации гостевые WLAN используют веб-аутентификацию для проверки пользователей, а защищенная внутренняя WLAN использует протокол расширенной аутентификации (EAP).

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем

попробовать эту конфигурацию:

- Знание способов настройки WLC с основными параметрами
- Знание способов настройки DHCP и сервера системы доменных имен (DNS)

Используемые компоненты

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

- Cisco 2006 WLC, использующий микропрограммное обеспечение версии 4.0
- LAP серии 1000 Cisco
- Беспроводной клиентский адаптер Cisco 802.11a/b/g, использующий микропрограммное обеспечение версии 2.6
- Маршрутизатор 2811 Cisco с использованием IOSB® Cisco версии 12.4(2)XA
- Коммутатор серии 3500 XL Cisco с использованием IOS Cisco версии 12.0(5)WC3b
- Сервер DNS, который используется сервером Microsoft Windows 2000

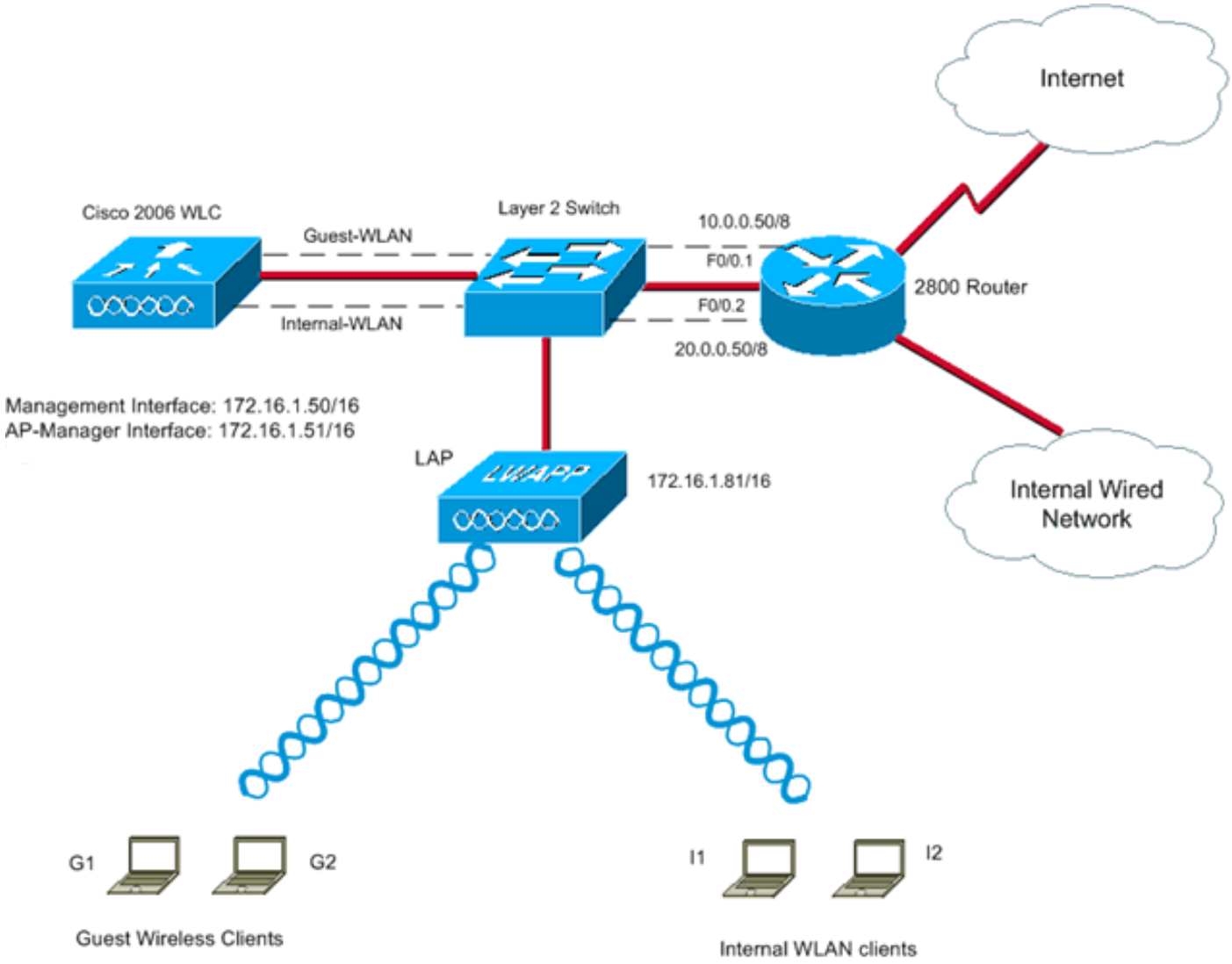
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка сети

Пример конфигурации в данном документе использует настройку, отображенную на данной схеме. LAP зарегистрирована на WLC. WLC подключен к коммутатору уровня 2. Маршрутизатор, который подключает пользователей к сети WAN, также подключается к коммутатору уровня 2. Необходимо создать две сети WLAN, для гостевых пользователей и для пользователей внутренней LAN. Также необходим сервер DHCP, чтобы обеспечить гостевые и внутренние беспроводные клиенты IP-адресами. Чтобы получить доступ к сети, гостевые пользователи используют веб-аутентификацию. Внутренние пользователи используют протокол аутентификации EAP. Для беспроводных клиентов маршрутизатор 2811 служит сервером DHCP.



Примечание: В данном документе предполагается, что WLC настроен с использованием основных параметров, а LAP зарегистрирован на WLC. Дополнительные сведения по настройке основных параметров на WLC и о регистрировании LAP на WLC см. в разделе Регистрация упрощенных точек доступа (LAP) на контроллере беспроводной локальной сети (WLC).

При настройке сервера DHCP, некоторые межсетевые экраны не поддерживают запросы DHCP от агента ретрансляции. Для клиента агентом ретрансляции является WLC. Межсетевой экран, настроенный в качестве сервера DHCP, игнорирует данные запросы. Клиенты должны быть напрямую подключены к межсетевому экрану, так как запросы не могут отсылаться через другой агент ретрансляции или маршрутизатор. Межсетевой экран может работать в качестве сервера DHCP для внутренних узлов, подключенных к нему напрямую. Это позволяет межсетевому экрану поддерживать свою таблицу, основанную на MAC-адресах, которые подключены напрямую и видны ему. Именно поэтому происходит сброс пакетов, а попытка назначить адреса от ретрансляции DHCP невыполнима. У межсетевого экрана PIX есть данное ограничение.

Настройка

Чтобы настроить устройство для данной конфигурации сети, выполните следующие действия:

1. Настройка динамических интерфейсов на WLC для гостевых и внутренних

пользователей
2. Создать сети WLAN для гостевых и внутренних пользователей
3. Настройте порт коммутатора уровня 2, который подключается к WLC в качестве магистрального порта
4. Настройте маршрутизатор для двух сетей VLAN

Настройка динамических интерфейсов на WLC для гостевых и внутренних пользователей

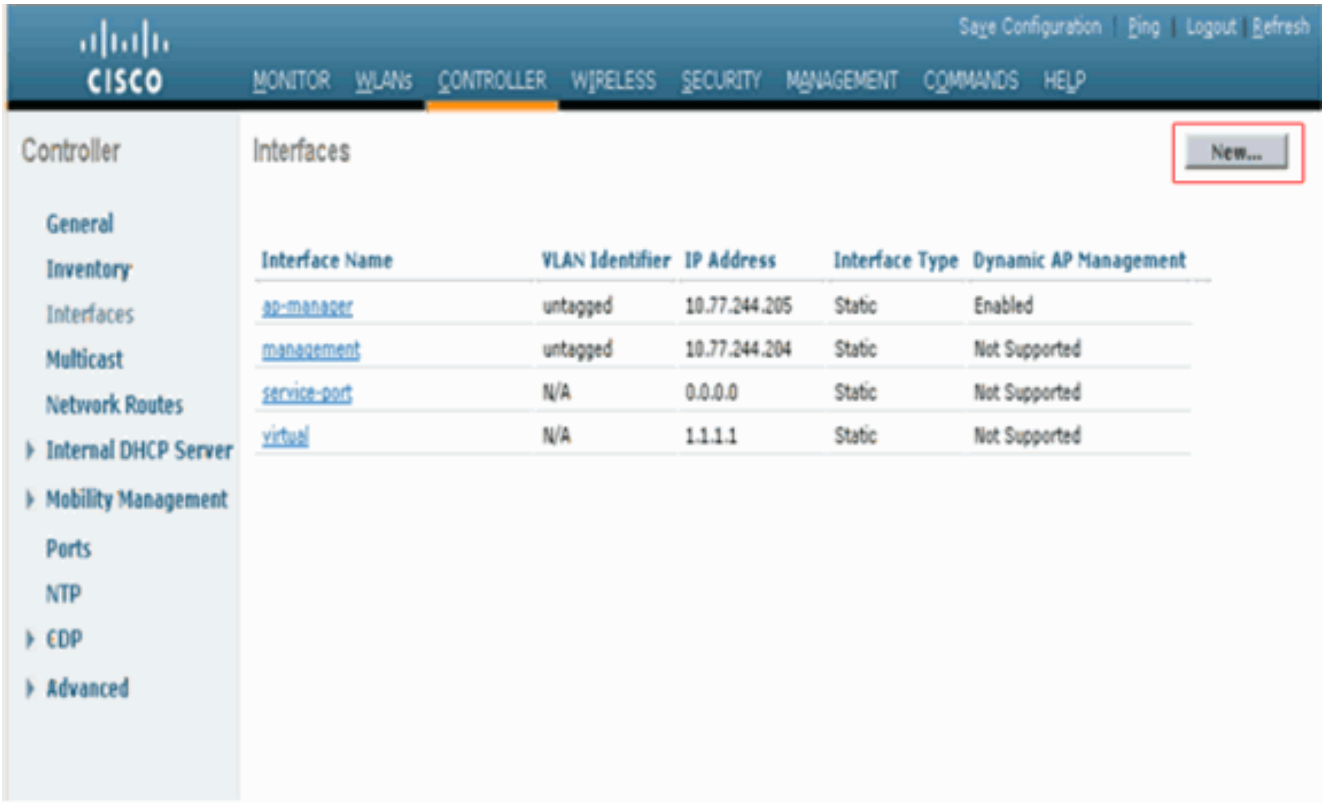
Прежде всего, на WLC создайте два динамических интерфейса, для гостевых и внутренних пользователей.

В примере данного документа для динамических интерфейсов используются следующие параметры и значения:

```
Guest-WLAN                                                    Internal-WLAN
VLAN Id : 10                              VLAN Id : 20
IP address: 10.0.0.10                        IP address: 20.0.0.10
Netmask: 255.0.0.0 Netmask: 255.0.0.0
Gateway: 10.0.0.50                          Gateway: 20.0.0.50
Physical port on WLC: 1                       Physical port on WLC: 1
DHCP server: 172.16.1.60                        DHCP server: 172.16.1.60
```

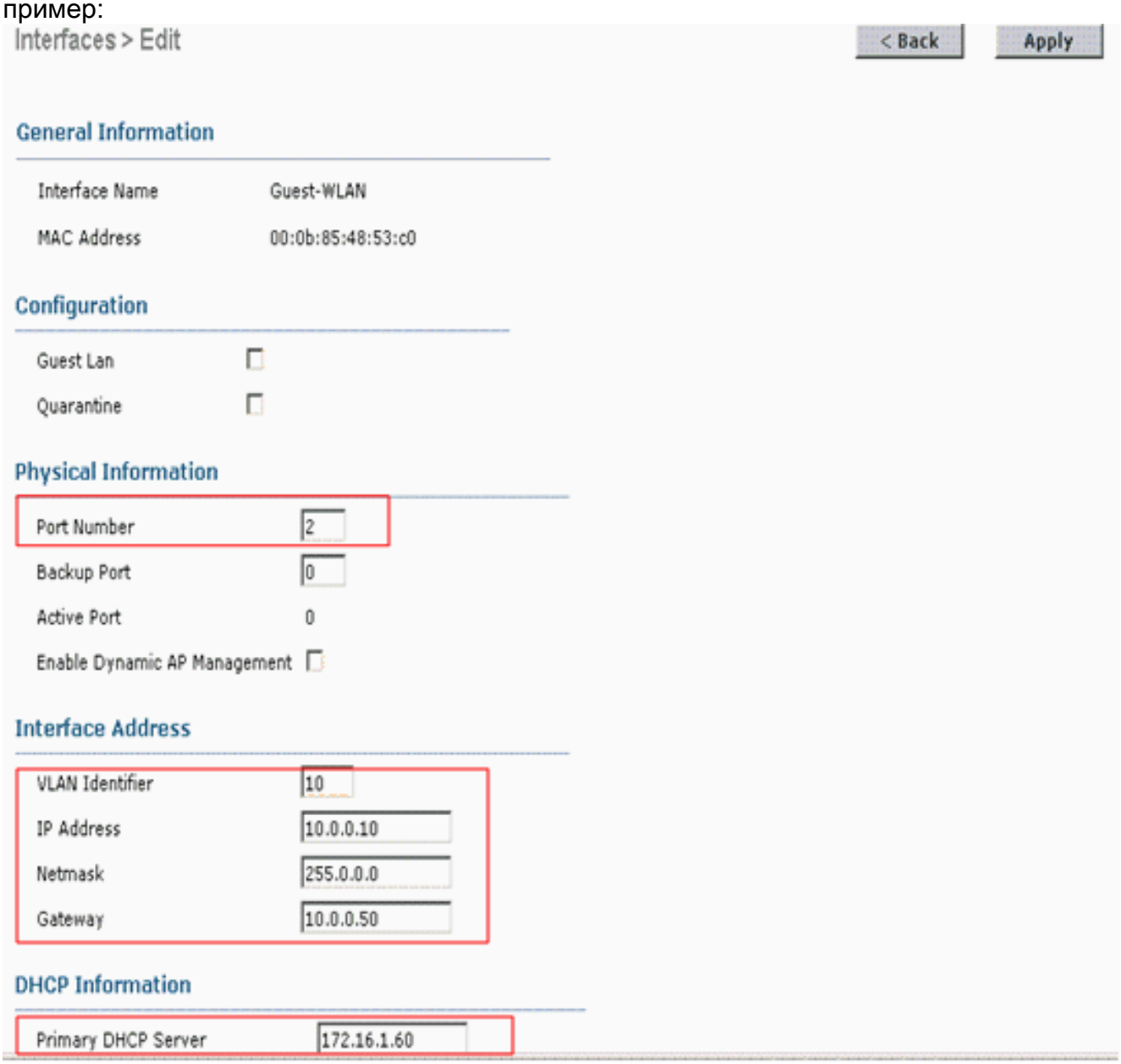
Выполните следующие действия:

1. **В графическом интерфейсе пользователя (GUI) WLC, выберите Controllers > Interfaces.**Отобразится окно интерфейсов. В окне отобразится список интерфейсов, настроенных для этого контроллера. Список включает в себя интерфейсы по умолчанию, в которые входят интерфейс управления, интерфейс диспетчера точки доступа, виртуальный интерфейс и интерфейс сервисного порта, а также динамические интерфейсы, определенные пользователями.



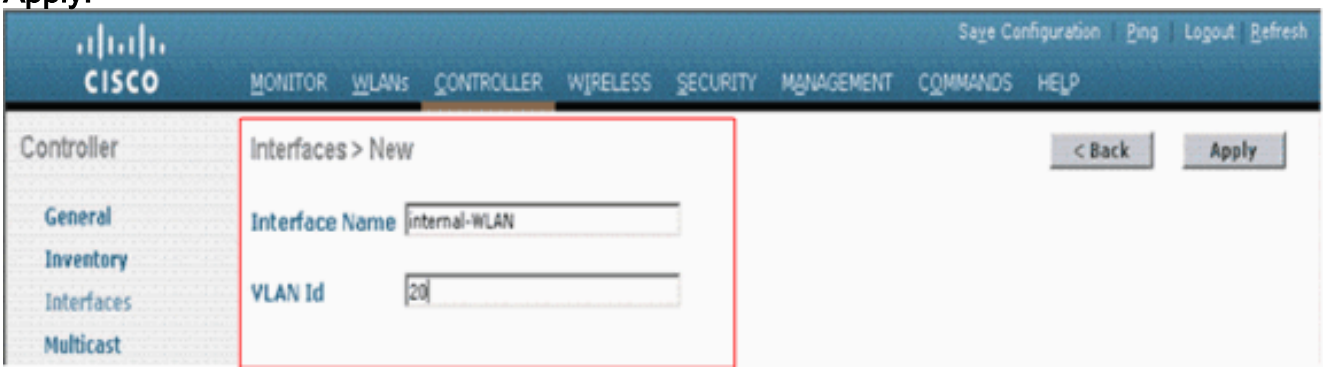
2. **Нажмите New, чтобы создать новый динамический интерфейс.**
3. **В окне Interfaces > New введите имя интерфейса и идентификатор VLAN. Нажмите кнопку Apply.**В данном примере динамический интерфейс назван Guest-WLAN, а идентификатору VLAN назначено
   10.

4. В окне Interfaces > Edit динамического интерфейса введите IP-адрес, маску подсети и шлюз по умолчанию. Назначьте его для физического порта контроллера беспроводной сети и укажите IP-адрес сервера DHCP. **Затем нажмите Apply.**Ниже представлен пример:

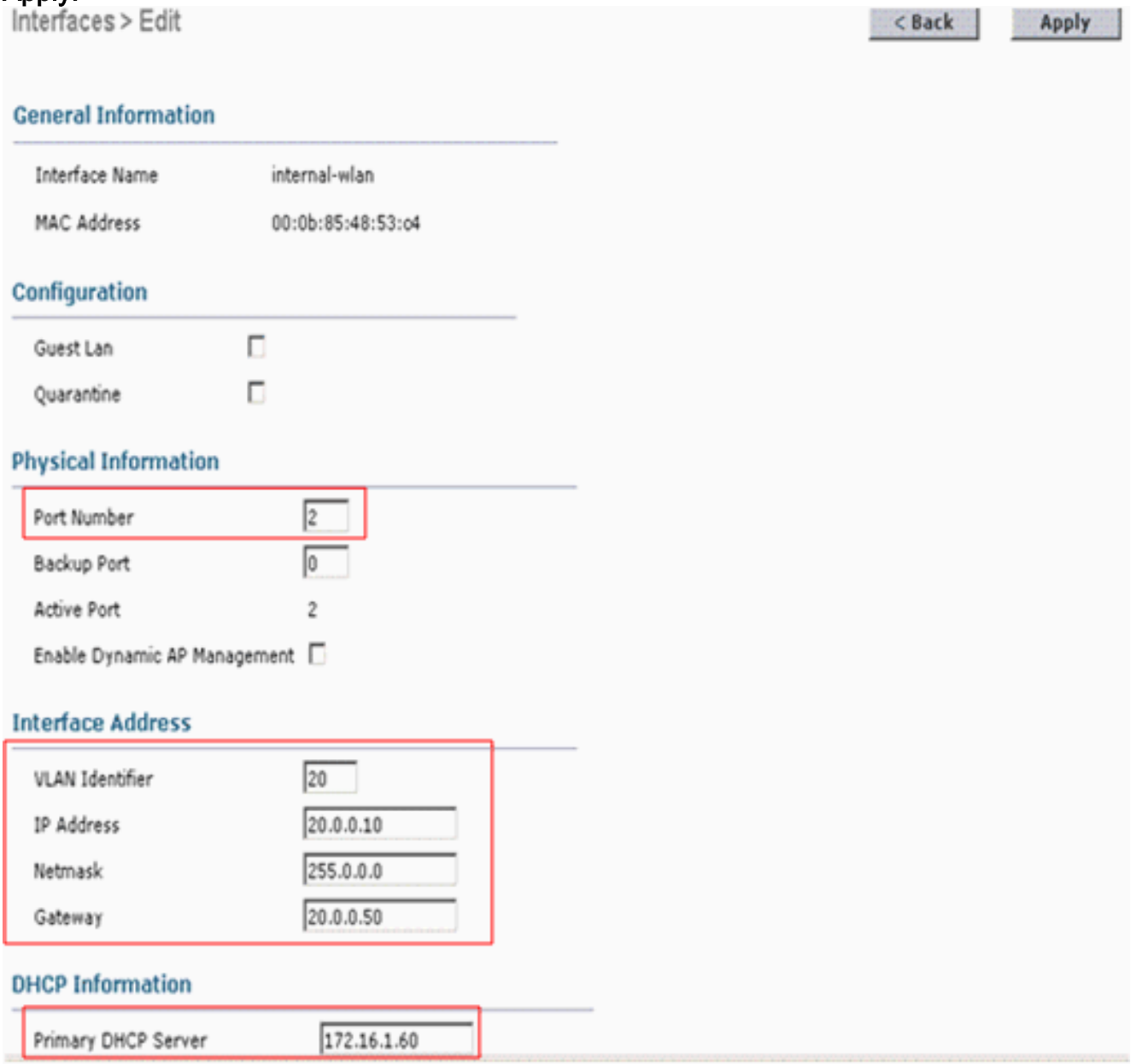


Чтобы создать динамический интерфейс для внутренней WLAN, необходимо выполнить такую же процедуру.

5. **В окне Interfaces > New динамического интерфейса введите Internal-WLAN для внутренних пользователей, а идентификатору VLAN задайте 20. Нажмите кнопку Apply.**



6. В окне Interfaces > Edit динамического интерфейса введите IP-адрес, маску подсети и шлюз по умолчанию. Назначьте его для физического порта контроллера беспроводной сети и укажите IP-адрес сервера DHCP. **Затем нажмите Apply.**



После создания двух динамических интерфейсов в окне "Interfaces" отображается сводный список интерфейсов, настроенных на контроллере.

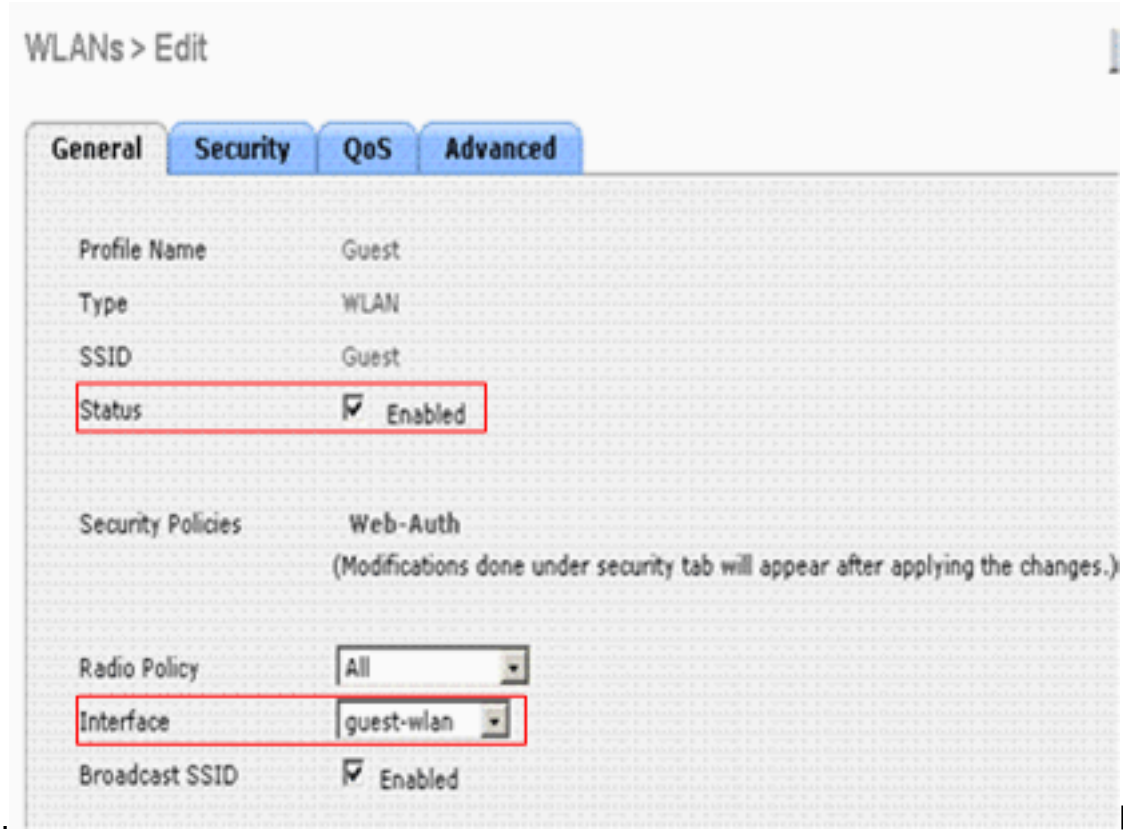
Создать сети WLAN для гостевых и внутренних пользователей

Следующий шаг – создание WLAN для гостевых и внутренних пользователей, и установление соответствия динамических интерфейсов в сетях WLAN. Должны быть определены методы обеспечения безопасности, используемые для аутентификации гостевых и беспроводных пользователей. Выполните следующие действия:

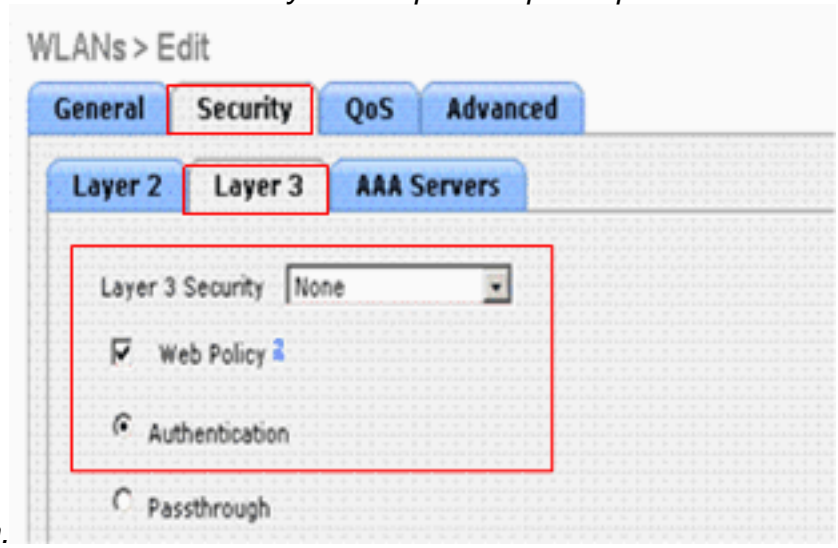
1. **Нажмите WLANs в графическом интерфейсе контроллера для создания WLAN.**Откроется окно WLAN. В данном окне находится список сетей WLAN, настроенных на контроллере.
2. **Нажмите New для настройки новой WLAN.***В данном примере имя для WLAN – Guest, а идентификатор сети (WLAN ID) –*

2.

3. Нажмите **Apply** в правом верхнем угле.
4. WLAN> экран Edit появляется, который содержит различные вкладки.Под **Вкладкой Общие** для гостевого WLAN выберите **гостя-wlan** из поля Interface Name. **Это устанавливает соответствие динамического интерфейса guest-wlan, которое было создано раньше на WLAN Guest.**Удостоверьтесь, что включен Статус

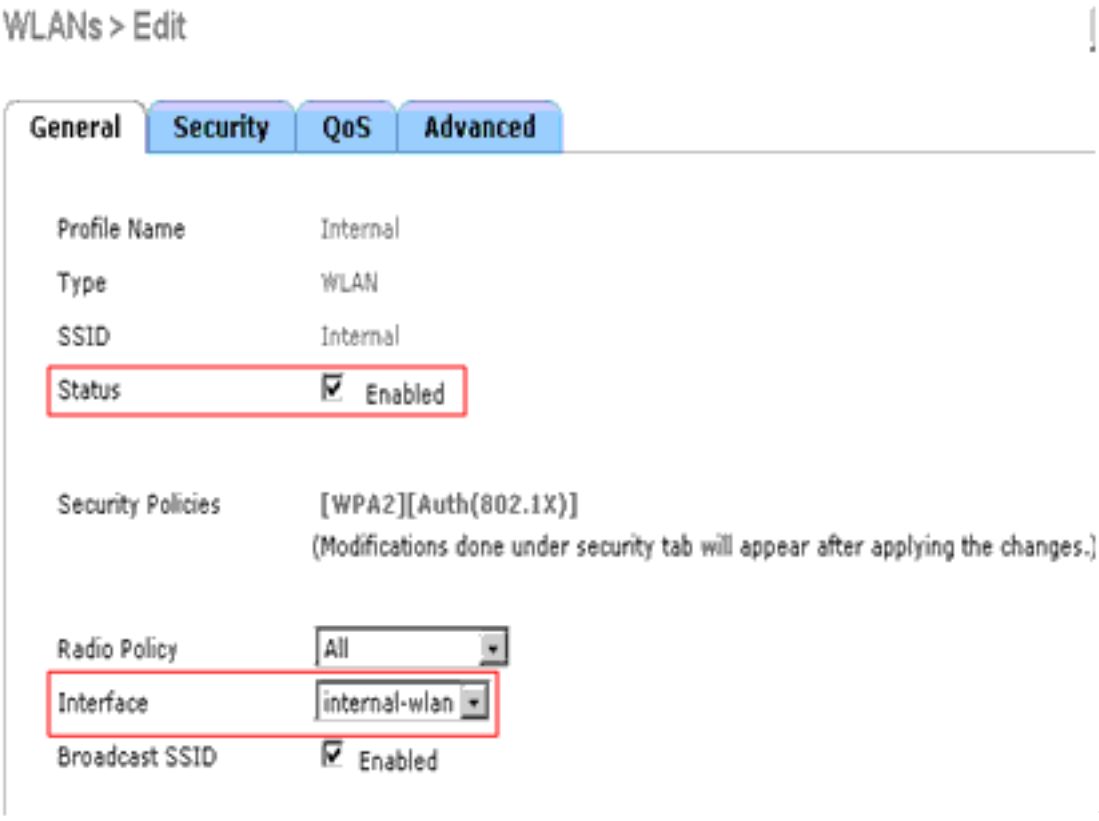


WLAN. **Щелкните вкладку Безопасность.** Для этого WLAN Web-аутентификация механизм безопасности уровня 3 используется для аутентификации клиентов. Поэтому выберите **None** под полем *безопасности уровня 2. В поле обеспечения безопасности 3 уровня установите флажок на Web Policy и выберите параметр*

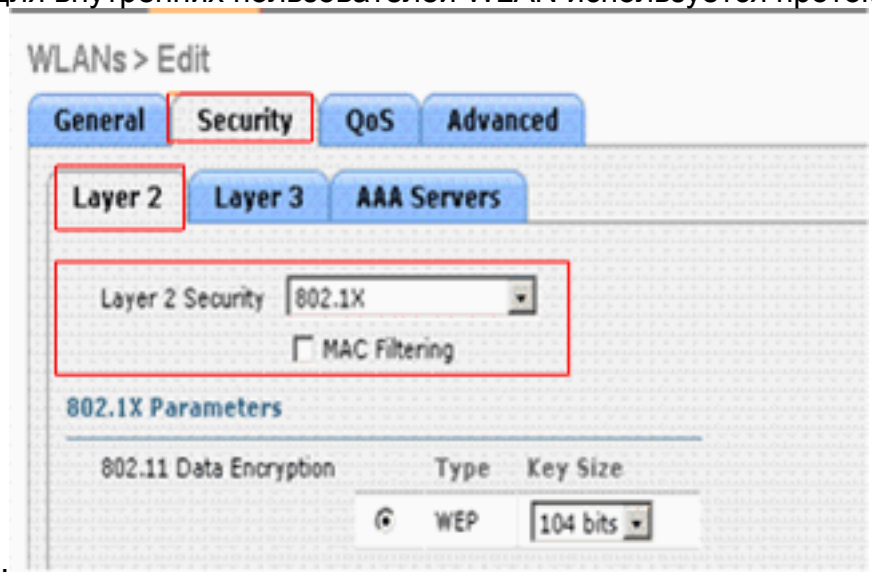


Authentication. **Примечание:** Для получения дополнительной информации о Web-аутентификации обратитесь к Примеру настройки веб-аутентификации в контроллере беспроводной сети LAN.**Щелкните "Применить".**

5. Создайте WLAN для внутренних пользователей. **Чтобы создать WLAN для внутренних пользователей, нажмите Internal и выберите 3 в окне WLANs > New. Затем нажмите Apply.**
6. WLAN> Окно редактирования появляются. Под *Вкладкой Общие* выберите **внутренний-wlan** из поля Interface Name.**Это устанавливает соответствие динамического интерфейса internal-wlan, которое было создано раньше на WLAN Internal.** Удостоверьтесь, что включен



WLAN. Значение 802.1x параметра обеспечения безопасности уровня 2 оставьте по умолчанию, так как для внутренних пользователей WLAN используется протокол аутентификации



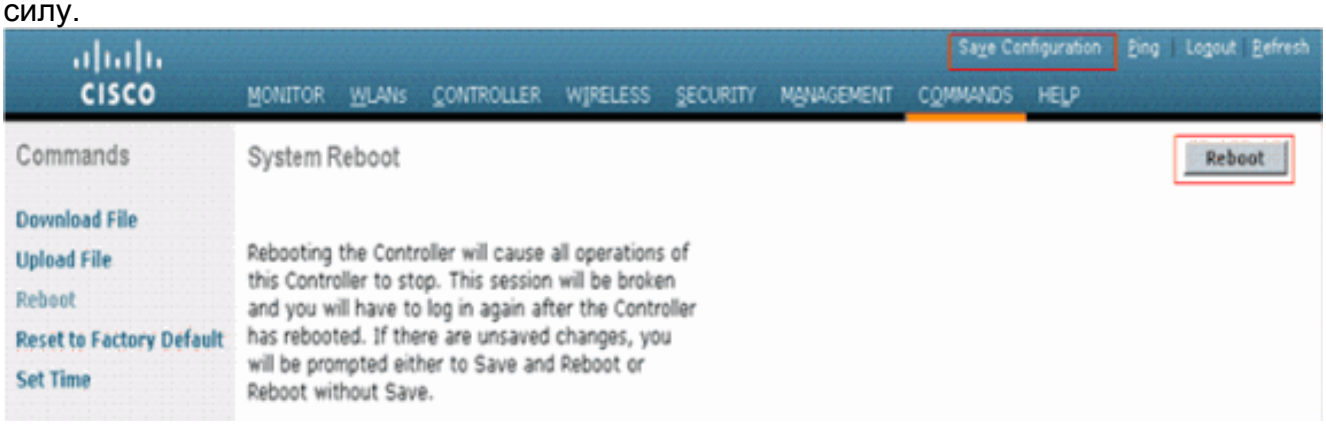
EAP.

7. **Щелкните "Применить".**Окно WLAN появляется, и оно показывает список WLAN, которые
созданы.

Примечание: [Дополнительные сведения по настройке WLAN по протоколу EAP при

использовании WLC, см. в разделе Пример настройки аутентификации EAP с помощью контроллеров WLAN (WLC).

8. На GUI WLC нажмите **Save Configuration**, затем нажмите **Commands** от графического интерфейса контроллера. Затем, выберите опцию **Reboot** для перезагрузки WLC, чтобы позволить web-аутентификации вступать в силу.



Примечание: Нажмите **Save Configuration** для сохранения конфигурации через перезагрузки.

Настройте порт коммутатора уровня 2, который подключается к WLC в качестве магистрального порта

Необходимо настроить порт коммутатора, который поддерживает несколько сетей VLAN настроенных на WLC, так как WLC подключен к коммутатору уровня 2. Порт коммутатора необходимо настроить в качестве магистрального порта 802.1Q.

Каждое соединение порта контроллера происходит на магистрали 802.1Q и должно быть настроено также на соседнем коммутаторе. На коммутаторах Cisco собственный VLAN магистрали "802.1q", например **VLAN 1**, оставляют без меток. Поэтому при настройке интерфейса контроллера для использования собственного VLAN на соседнем коммутаторе Cisco, удостоверьтесь, что вы настраиваете интерфейс на контроллере как без меток.

Нулевое значение для идентификатора VLAN (в окне Controller > Interfaces) означает, что интерфейс не помечен. В примере, приведенном в данном документе, менеджер точки доступа и интерфейсы управления настроены в непомеченной сети VLAN по умолчанию.

Когда интерфейс контроллера установлен в ненулевое значение, он не должен быть помечен к собственному VLAN коммутатора, и VLAN должна быть позволена на коммутаторе. В данном примере сеть VLAN 60 настроена в качестве исходной VLAN для порта коммутатора, который подсоединяется к контролеру.

Ниже приведена конфигурация для порта коммутатора, который подключается к WLC:

```
interface f0/12
Description Connected to the WLC
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

Ниже приведена конфигурация для порта коммутатора, который подключается к маршрутизатору в качестве магистрального порта:

```
interface f0/10
Description Connected to the Router
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport trunk allowed vlan 10,20,60
switchport mode trunk
no ip address
```

Ниже приведена конфигурация для порта коммутатора, который подсоединяется к LAP. Данный порт настроен в качестве порта доступа:

```
interface f0/9
Description Connected to the LAP
Switchport access vlan 60
switchport mode access
no ip address
```

Настройка маршрутизатора для двух WLAN

В примере, приведенном в данном документе, маршрутизатор 2811 подключает гостевых пользователей к Интернету, а также проводных внутренних пользователей к внутренним беспроводным пользователям. Необходимо настроить маршрутизатор для предоставления служб DHCP.

На маршрутизаторе создайте подчиненные интерфейсы под Интерфейсом Fast Ethernet, который соединяется с магистральным портом на коммутаторе для каждой VLAN. Назначьте подчиненные интерфейсы на соответствующие VLAN и настройте IP-адрес от соответствующих подсетей.

Примечание: Дана только важная часть конфигурации маршрутизатора, а не полная конфигурация.

Это необходимая конфигурация маршрутизатора.

Ниже приведены команды, необходимые для настройки служб DHCP на маршрутизаторе:

```
!
ip dhcp excluded-address 10.0.0.10
!--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC.
ip dhcp excluded-address 10.0.0.50 !--- IP excluded because this IP is assigned to the !--- sub-interface on the router. ip dhcp excluded-address 20.0.0.10 !--- IP excluded because this IP is assigned to the dynamic !--- interface created on the WLC. ip dhcp excluded-address 20.0.0.50 !--- IP excluded because this IP is assigned to the sub-interface on the router. ! ip dhcp pool Guest !--- Creates a DHCP pool for the guest users. network 10.0.0.0 255.0.0.0 default-router 10.0.0.50 dns-server 172.16.1.1 !--- Defines the DNS server. ! ip dhcp pool Internal network 20.0.0.0 255.0.0.0 default-router 20.0.0.50 !--- Creates a DHCP pool for the internal users. !
```

Данные команды должны быть выполнены на интерфейсе FastEthernet для настройки, показанной в примере:

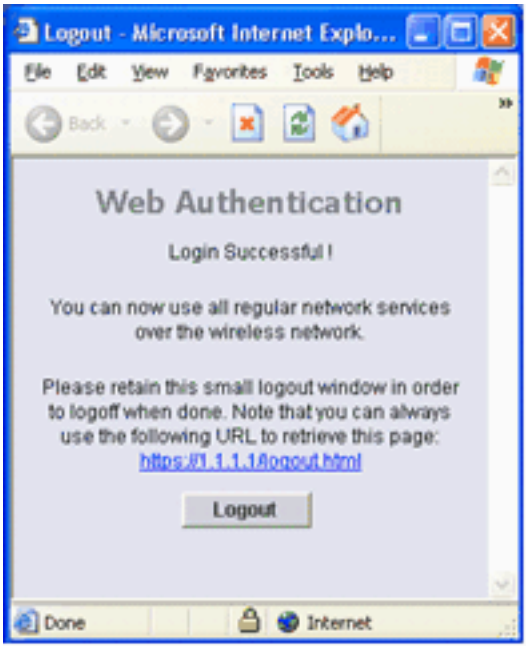
```
!
interface FastEthernet0/0
 description Connected to L2 Switch
 ip address 172.16.1.60 255.255.0.0
 duplex auto
 speed auto
!--- Interface connected to the Layer 2 switch. ! interface FastEthernet0/0.1 description Guest VLAN encapsulation dot1Q 10 ip address 10.0.0.50 255.0.0.0 !--- Creates a sub-interface under FastEthernet0/0 for the guest VLAN. ! interface FastEthernet0/0.2 description Internal VLAN encapsulation dot1Q 20 ip address 20.0.0.50 255.0.0.0 !--- Creates a sub-interface under FastEthernet0/0 for the internal VLAN. !
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

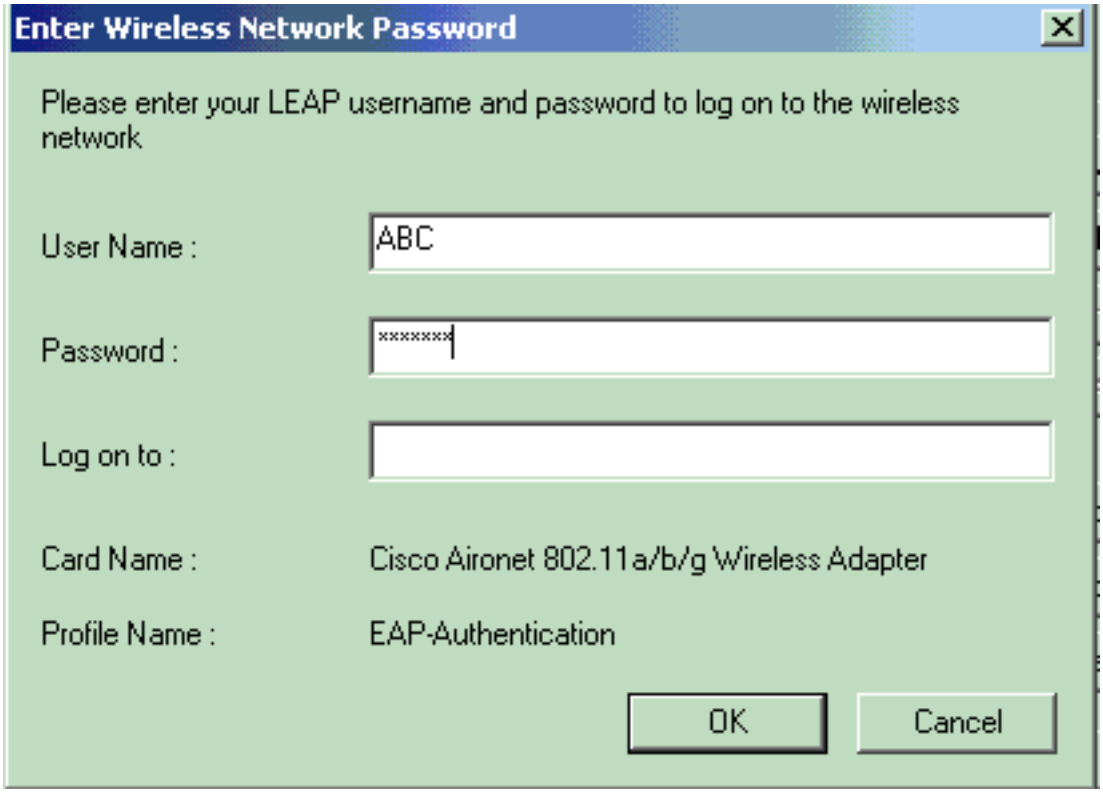
Подключите два беспроводных клиента, гостевого пользователя (с идентификатором набора служб [SSID] Guest) и внутреннего пользователя (с идентификатором SSID Internal), чтобы проверить, что конфигурация работает, как положено.

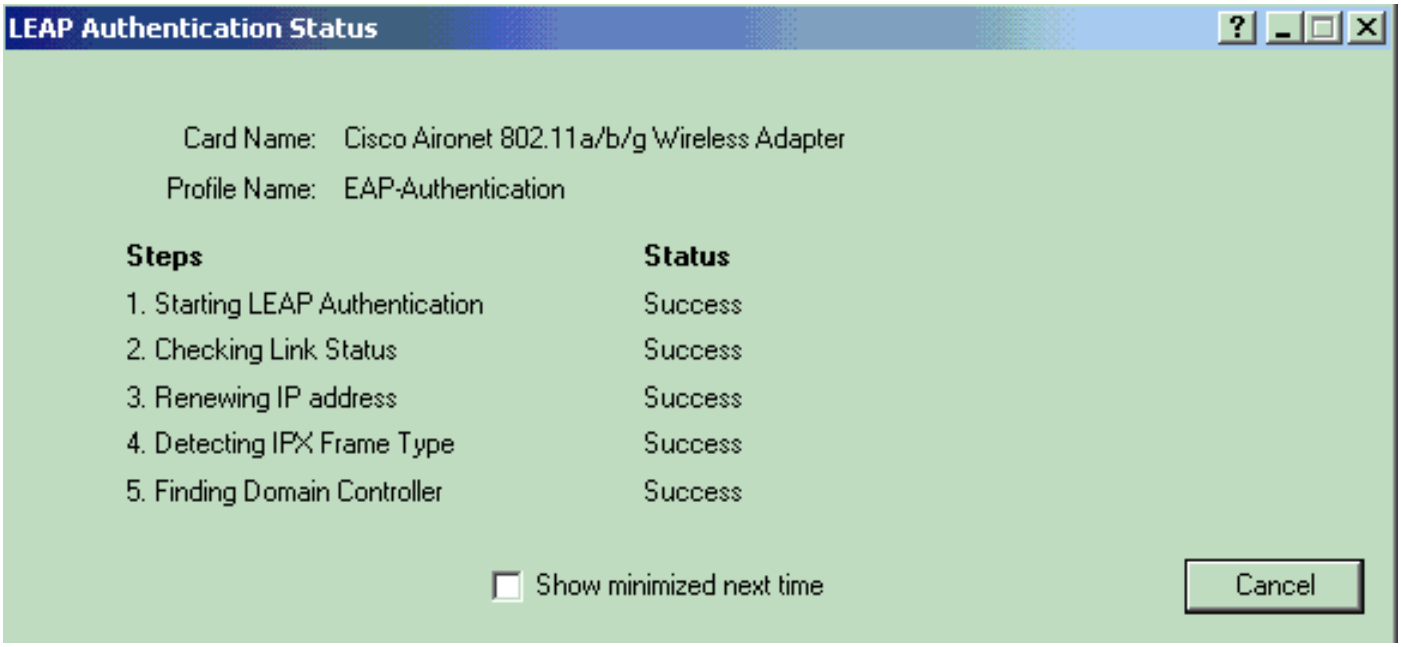
Помните, что гостевой WLAN был настроен для Web-аутентификации. После загрузки гостевого беспроводного клиента, в веб-браузере введите любой URL. Страница аутентификации веб-страницы по умолчанию появляется и побуждает вас вводить имя пользователя и пароль. Как только гостевой пользователь введет действующее имя пользователя и пароль, WLC аутентифицирует гостевого пользователя и разрешит доступ к сети (возможно к Интернет). Данный пример показывает окно веб-аутентификации, которую получает пользователь и выходные данные по успешной аутентификации:



Внутренний WLAN в данном примере настроен для аутентификации 802.1x. После загрузки

внутреннего WLAN клиента используется аутентификация протокола EAP. Для получения дополнительной информации о том, как настроить клиента для Аутентификации eap, обратитесь к Использованию раздела Аутентификации eap Cisco Aironet 802.11a/b/g Клиентские адаптеры беспроводной сети (CB21AG и PI21AG) Руководство по установке и конфигурированию. Если аутентификация прошла успешно, пользователь получает доступ к внутренней сети. Данный пример показывает внутреннего беспроводного клиента, который использует упрощенный расширяемый протокол аутентификации (LEAP):





Устранение неполадок

Процедура устранения неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Если конфигурация работает ненадлежащим образом, выполните следующие действия:

1. Убедитесь, что все сети VLAN настроенные на WLC разрешены на порте коммутатора, подключенного к WLC.
2. Убедитесь, что подключенный к WLC и маршрутизатору, порт коммутатора настроен в качестве магистрального порта.
3. Проверьте, что на WLC и маршрутизаторе используются одинаковые идентификаторы сети VLAN.
4. Проверьте получение DHCP адресов клиентом с сервера DHCP. Если нет, проверьте правильность настройки DHCP сервера. Для получения дополнительной информации об устранении проблем клиентов выдал обратитесь к Устранению проблем Клиентов выдал в единой беспроводной сети Cisco (UWN).

Одна из часто встречаемых проблем, связанных с веб-аутентификацией, заключается в перенаправлении на несуществующую страницу веб-аутентификации. Когда пользователь открывает веб-браузер, он не видит окна веб-аутентификации. **Вместо этого пользователю необходимо вручную ввести https://1.1.1.1/login.html, чтобы открыть окно веб-аутентификации.** Это связано с поиском в DNS, который необходимо выполнить перед тем, как произойдет перенаправление на страницу веб-аутентификации. Если в адресе домашней страницы веб-браузера беспроводного клиента указывается имя домена, должна быть возможность успешного выполнения команды nslookup после привязки клиента, чтобы перенаправление работало.

Кроме того, на контроллерах WLC с программным обеспечением версий, предшествующих 3.2.150.10, веб-аутентификация работает следующим образом: когда пользователь с заданным SSID пытается получить доступ к Интернету, интерфейс управления контроллера отправляет DNS-запрос, чтобы проверить допустимость URL-адреса. В случае успешной проверки отображается URL страница проверки подлинности с IP-адресом виртуального интерфейса. После успешной регистрации пользователя исходному запросу разрешается вернуться к клиенту. Обратитесь к сообщению об ошибке Cisco с идентификатором CSCsc68105 (только для зарегистрированных пользователей) . Для получения дополнительной информации обратитесь к Устранению проблем Web-аутентификации на Контроллере беспроводной локальной сети (WLC).

Команды для устранения неполадок

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

Можно использовать эти команды debug для устранения неисправностей конфигурации:

- **debug mac addr <MAC-адрес клиента xx:xx:xx:xx:xx:xx> - настраивает отладку MAC-адреса для клиента.**
- **debug aaa all enable – настраивает отладку сообщений AAA.**
- **debug pem state enable - настраивает отладку конечного автомата менеджера политик.**
- **debug pem events enable - настраивает отладку событий менеджера политик.**
- **debug dhcp message enable – используйте эту команду для отображения отладочной информации об активности пользователей в отношении протокола (DHCP) и контроля состояний пакетов DHCP.**
- **debug dhcp packet enable - используйте эту команду для отображения информации пакетного уровня DHCP.**

- debug pm ssh-appgw enable - настраивает отладку шлюзов приложений.
- debug pm ssh-tcp enable – настраивает отладку обработки пакетов TCP менеджера политик.

Ниже приведен пример выходных данных некоторых команд debug:

Примечание: Некоторые строки выходных данных были перемещены на вторую строку из-за нехватки пространства.

(Cisco Controller) >debug dhcp message enable Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: **requested ip = 10.0.0.1** Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: vendor class id = MSFT5.0 (len 8) Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 Forwarding DHCP packet (332 octets)from 00:40:96:ac:e6:57 -- packet received on direct-connect port requires forwarding to external DHCP server. Next-hop is 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50 Fri Mar 2 16:01:43 2007: 00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64

(Cisco Controller) >debug dhcp packet enable Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1, encap: 0xec03 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request, client: 00:40:96:ac:e6:57: dhcp op: 1, port: 2, encap 0xec03, old mscb port number: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay for 00:40:96:ac:e6:57 dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50, dhcpRelay: 10.0.0.10 VLAN: 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57 Local Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50, VLAN: 30, port: 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREQUEST, htype: Ethernet,hlen: 6, hops: 1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 10.0.0.10 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50, len 350,switchport 2, vlan 30 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREPLY(2), IP len: 300, switchport: 2, encap: 0xec00 Fri Mar 2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57, frame len412, switchport 2 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP ACK msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr: 10.0.0.1 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 0.0.0.0 Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1 rcvd server id: 10.0.0.50

(Cisco Controller) >debug aaa all enable Fri Mar 2 16:22:40 2007: **User user1 authenticated** Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 **Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57** Fri Mar 2 16:22:40 2007: AuthorizationResponse: 0xbadff97c Fri Mar 2 16:22:40 2007: structureSize.....70 Fri Mar 2 16:22:40 2007: resultCode.....0 Fri Mar 2 16:22:40 2007: protocolUsed.....0x00000008 Fri Mar 2 16:22:40 2007: proxyState.....00:40:96:AC:E6:57-00:00 Fri Mar 2 16:22:40 2007: Packet contains 2 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] Service-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2

16:22:40 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48, valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: Fri Mar 2 16:22:40 2007: 00:40:96:ac:e6:57 Unable to apply override policy for station 00:40:96:ac:e6:57 - VapAllowRadiusOverride is FALSE Fri Mar 2 16:22:40 2007: AccountingMessage Accounting Start: 0xa62700c Fri Mar 2 16:22:40 2007: Packet contains 13 AVPs: Fri Mar 2 16:22:40 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:22:40 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:22:40 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:22:40 2007: AVP[11] Acct-Status-Type.....0x00000001 (1) (4 bytes) Fri Mar 2 16:22:40 2007: AVP[12] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:22:40 2007: AVP[13] Called-Station-Id.....10.77.244.210 (13 bytes) when web authentication is closed by user: (Cisco Controller) >Fri Mar 2 16:25:47 2007: AccountingMessage Accounting Stop: 0xa627c78 Fri Mar 2 16:25:47 2007: Packet contains 20 AVPs: Fri Mar 2 16:25:47 2007: AVP[01] User-Name.....user1 (5 bytes) Fri Mar 2 16:25:47 2007: AVP[02] Nas-Port.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[03] Nas-Ip-Address.....0x0a4df4d2 (172881106) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[04] NAS-Identifier.....0x574c4331 (1464615729) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[05] Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[06] Acct-Session-Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes) Fri Mar 2 16:25:47 2007: AVP[07] Acct-Authentic.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[08] Tunnel-Type.....0x0000000d (13) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[09] Tunnel-Medium-Type.....0x00000006 (6) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[10] Tunnel-Group-Id.....0x3330 (13104) (2 bytes) Fri Mar 2 16:25:47 2007: AVP[11] Acct-Status-Type.....0x00000002 (2) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[12] Acct-Input-Octets.....0x0001820e (98830) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[13] Acct-Output-Octets.....0x00005206 (20998) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[14] Acct-Input-Packets.....0x000006ee (1774) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[15] Acct-Output-Packets.....0x00000041 (65) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[16] Acct-Terminate-Cause.....0x00000001 (1) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[17] Acct-Session-Time.....0x000000bb (187) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[18] Acct-Delay-Time.....0x00000000 (0) (4 bytes) Fri Mar 2 16:25:47 2007: AVP[19] Calling-Station-Id.....10.0.0.1 (8 bytes) Fri Mar 2 16:25:47 2007: AVP[20] Called-Station-Id.....10.77.244.210 (13 bytes) **(Cisco Controller) >debug pem state enable** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **WEBAUTH_REQD (8) Change state to START (0)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 **AUTHCHECK (2) Change stateto L2AUTHCOMPLETE (4)** Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_NOL3SEC (14) Change state to RUN (20) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) Fri Mar 2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1 DHCP_REQD (7) Change stateto RUN (20) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4) Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change

state to DHCP_REQD (7) Fri Mar 2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2 DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)

(Cisco Controller) >debug pem events enable Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policy Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Replacing Fast Path rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Deleting mobile policy rule 27 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web RuleID 28 for mobile 00:40:96:ac:e6:57 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding TMP rule Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) ReplacingFast Path rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255) Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry. Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8 Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8

Дополнительные сведения

- Часто задаваемые вопросы о беспроводном доступе гостя
- Пример конфигурации гостевого доступа к проводной сети с использованием контроллеров WLAN Cisco
- Примеры настройки аутентификации на контроллерах беспроводной сети LAN
- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация