

Использование VLAN с беспроводным оборудованием Cisco Aironet

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Родственные продукты](#)

[Условные обозначения](#)

[VLAN](#)

[Значение собственной VLAN](#)

[Точки доступа VLAN](#)

[Сведения о точках доступа VLAN](#)

[Настройка точки доступа](#)

[VLAN на мостах](#)

[Сведения о мостах](#)

[Настройка моста](#)

[Используйте сервер RADIUS для присвоения пользователей на VLAN](#)

[Используйте сервер RADIUS для динамического присвоения группы мобильности](#)

[Конфигурация группы мостов на точках доступа и мостах](#)

[Concurrent Routing and Bridging \(IRB\)](#)

[Взаимодействие с родственными коммутаторами](#)

[Конфигурация коммутатора—ОС Catalyst](#)

[Настройка коммутатора — Коммутаторы Catalyst на основе операционной системы IOS](#)

[Настройка коммутатора в Ъ Catalyst 2900XL/3500XL](#)

[Проверка](#)

[Проверка беспроводного оборудования](#)

[Проверить коммутатор](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

[Введение](#)

Данный документ содержит пример настройки для использования виртуальных локальных сетей (VLAN) с беспроводным оборудованием Cisco Aironet.

[Предварительные условия](#)

Требования

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

- Знакомство с беспроводным оборудованием Cisco Aironet
- Знакомство с понятиями коммутации LAN VLAN и транкинга VLAN

Используемые компоненты

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

- Точки доступа Aironet Access и беспроводные мосты
- Коммутаторы Cisco Catalyst

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.

Родственные продукты

Можно использовать сторону коммутатора этой конфигурации с любым из них аппаратные средства или программное обеспечение:

- Catalyst 6x00/5x00/4x00, который выполняет CatOS или IOS
- Catalyst 35x0/37x0/29xx, который выполняет IOS
- Catalyst 2900XL, который выполняет IOS

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

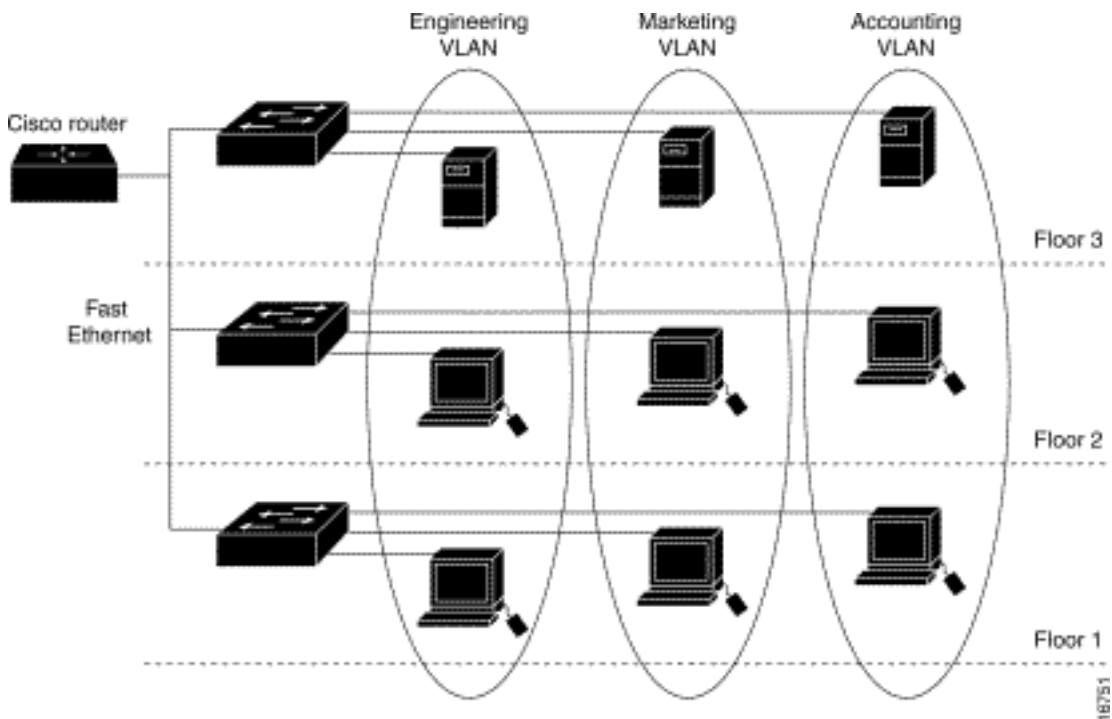
VLAN

VLAN является коммутируемой сетью, которая логически сегментирована функциями, проектными группами или приложениями, а не на медосмотре или географической основе. Например, все рабочие станции и серверы, используемые определенной командой рабочей группы, могут быть связаны с той же VLAN, независимо от их физических соединений к сети или факту, что они могут быть смешаны с другими командами. Используйте VLAN, чтобы реконфигурировать сеть через программное обеспечение, а не физически отключить или переместить устройства или провода.

VLAN может считаться широкоэмитательным доменом, который существует в определенном наборе коммутаторов. VLAN состоит из многих конечных систем, или хосты или сетевое оборудование (такие как мосты и маршрутизаторы), связанный одиночным доменом соединения. Домен соединения поддерживается на различных частях сетевого оборудования, таких как коммутаторы локальной сети (LAN), которые управляют

протоколами привязки между ними с отдельной группой для каждой VLAN.

При соединении устройства с коммутатором Cisco Catalyst порт, где устройство связано, является членом LAN 1. MAC-адрес данного устройства входит в состав VLAN 1. На одном коммутаторе можно определить несколько виртуальных локальных сетей, и на большинстве моделей коммутаторов Catalyst можно сконфигурировать принадлежность порта коммутатора сразу нескольким VLAN.



Если число портов в сети превышает число портов коммутатора, то необходимо выполнить кросс-коммутацию нескольких стоек коммутаторов, которые образуют магистраль. Магистраль не принадлежит какой-либо сети VLAN, однако она является средством передачи трафика для одной или нескольких сетей VLAN.

В фундаментальных сроках ключ в конфигурации точки доступа для соединения с определенной VLAN должен настроить свой SSID для распознавания той VLAN. Поскольку VLAN определены ИДЕНТИФИКАТОРОМ VLAN или названием, из этого следует, что, если SSID на точке доступа настроен для распознавания определенного ИДЕНТИФИКАТОРА VLAN или названия, установлено соединение с VLAN. Когда это соединение сделано, связанные беспроводные клиентские устройства, которые имеют тот же SSID, могут обратиться к VLAN через точку доступа. VLAN обрабатывает данные к и от клиентов тот же способ, которым это обрабатывает данные к и от проводных соединений. Можно настроить до 16 SSIDs на точке доступа, таким образом, можно поддерживать до 16 VLAN. Можно назначить только один SSID на VLAN.

Когда вы добавляете осведомленность метки IEEE 802.11Q к точке доступа, вы расширяете VLAN в беспроводную локальную сеть. Кадры, предназначенные для других VLAN, переданы точкой доступа с помощью беспроводных технологий на другом SSIDs с другими ключами WEP. Только клиенты, привязанные к той VLAN, получают те пакеты. С другой стороны пакеты, которые прибывают от клиента, привязанного к определенной VLAN, 802.11Q теговые, прежде чем они будут переданы на проводную сеть.

Например, персонал и гости могут одновременно получить административно отдельный доступ к беспроводной сети компании. Виртуальная локальная сеть отображается на SSID, а беспроводной клиент подключается к соответствующему SSID. В сетях с беспроводными

мостами можно достигнуть нескольких VLAN через беспроводной канал для того, чтобы обеспечить возможности подключения к VLAN из отдельных точек доступа.

Если 802.1q настроен на Интерфейсе Fast Ethernet точки доступа, точка доступа всегда передает пакеты Keepalive на VLAN1, даже если VLAN 1 не определен на точке доступа. В результате Коммутатор Ethernet соединяется с точкой доступа и генерирует предупреждающее сообщение. Нет никакой потери функции или на точке доступа или на коммутаторе, но журнал коммутатора содержит бессмысленные сообщения, которые могут заставить более важные сообщения быть обернутыми и не замеченными.

Когда все SSIDs на точке доступа привязаны к сетям мобильной связи, это поведение создает проблему. Если все SSIDs привязаны к сетям мобильной связи, Порт коммутатора Ethernet, с которым связана точка доступа, может быть настроен как порт доступа. Порт доступа обычно назначается на собственный VLAN точки доступа, которая является не обязательно VLAN1. Это заставляет Коммутатор Ethernet генерировать предупреждающие сообщения, обращающие внимание, что трафик с 802.1q метка передается от точки доступа.

Можно устранить чрезмерные сообщения на коммутаторе при отключении функции поддержки активности.

Несоблюдение рекомендаций при развертывании сетей VLAN с беспроводным оборудованием Cisco Aironet может привести, например, к следующему нежелательному поведению:

- Не удалось ограничить количество допустимых VLAN на магистрали до количества, указанного для беспроводного устройства. Если на коммутаторе определены VLAN 1, 10, 20, 30 и 40, но только VLAN 1, 10 и 30 определены на беспроводном оборудовании, необходимо удалить все остальные сети из магистрали порта коммутатора.
- Неправильное употребление SSID обозначения инфраструктуры. Когда вы устанавливаете точки доступа, только назначаете SSID инфраструктуры при использовании SSID на: устройства моста рабочей группы точки доступа повторителя некорневой мосты. Это - неверная конфигурация для обозначения SSID инфраструктуры для SSID с только беспроводными переносными компьютерами для клиентов и вызывает непредсказуемые результаты. В установках моста можно использовать только одну инфраструктуру SSID. Инфраструктура SSID должна коррелировать с Native VLAN.
- Неправильное употребление или неправильный дизайн обозначения SSID гостевого режима. В случае указания нескольких SSID/VLAN на беспроводном оборудовании Cisco Aironet, один (1) SSID может быть назначен в гостевом режиме с вещанием SSID в радиомаяках 802.11. Другие SSID не являются широкоэмиттерными. Клиентские устройства должны указывать, какой SSID следует использовать для подключения.
- Ошибка при распознавании того, что несколько сетей VLAN и идентификаторов SSID указывают на несколько подсетей модели OSI уровня 3. Устаревшие версии программного обеспечения Cisco Aironet разрешают связывать множественный SSIDs с одной VLAN. Текущие версии эту возможность не поддерживают.
- Ошибки маршрутизации Уровня 3 Модели OSI или неправильные дизайны. Каждый SSID и его связанная VLAN должны иметь устройство маршрутизации и некоторый источник для адресации к клиентам, например сервер DHCP или область на сервере DHCP.
- Неправильно поймите или неправильно настройте Собственный VLAN. Маршрутизаторы

и коммутаторы, которые образуют физическую инфраструктуру сети, управляются иным способом, чем клиентские компьютеры, которые прикреплены к данной физической инфраструктуре. Сеть VLAN, членами которой являются интерфейсы маршрутизатора и коммутатора, называется собственной VLAN (по умолчанию, VLAN 1). Клиентские компьютеры являются членами другой VLAN, а IP-телефоны являются членами ещё одной VLAN. Управляющий интерфейс точки доступа или моста (интерфейс BVI1) считается и учитывается как часть собственной виртуальной локальной сети, независимо от того, какие VLAN или SSID проходят через это беспроводное устройство.

Значение собственной VLAN

При использовании магистрального порта соответствующего стандарту IEEE 802.1Q, всем фреймам назначаются метки кроме тех, которые в VLAN настроены как "native VLAN" для этого порта. В собственной VLAN фреймы всегда передаются немечеными и получают их тоже обычно немечеными. Таким образом, когда AP подключается к порту коммутатора, собственная VLAN, настраиваемая на AP, должна согласовываться с собственной VLAN, настроенной на порте коммутатора.

Примечание: Если существует рассогласование собственных VLAN, то фреймы будут отклоняться.

Этот сценарий необходимо пояснить на примере. Если собственная VLAN на порте коммутатора настраивается в качестве VLAN 12, а на AP собственная VLAN настраивается в качестве VLAN 1, то затем, когда AP отправляет какой-либо фрейм на его собственную VLAN в коммутаторе, коммутатор рассматривает фрейм как принадлежащий VLAN 12, так как фрейм из собственной VLAN на AP не имеет меток. Это является причиной дезорганизации работы сети и приводит к проблемам соединения. То же самое происходит в случаях, когда порт коммутатора направляет фрейм из собственной VLAN в AP.

Конфигурация собственной VLAN становится более важной, чем установка повторителя AP в беспроводной сети. Нельзя настроить несколько VLAN на повторителе AP. Повторитель AP поддерживает работу только с собственной VLAN. Таким образом, настройки собственной VLAN на корневой AP, порте коммутатора, к которому подключается AP, и повторителе AP должны быть теми же самыми. В противном случае трафик, проходящий через коммутатор, не будет передаваться на повторитель AP и не будет приниматься от него.

Примером сценария, когда рассогласованность настроек собственной VLAN повторителя AP может создать проблемы, является ситуация, при которой DHCP-сервер находится за коммутатором, к которому подключена корневая AP. В этом случае клиенты, связанные с повторителем AP, не получают IP-адрес от DHCP-сервера, так как фреймы отклоняются (в нашем случае DHCP-запросы), если они получены от собственной VLAN повторителя AP (не совпадает для корневого AP и коммутатора).

Кроме того, при настройке порта коммутатора убедитесь, что все VLAN, настроенные на AP, разрешены на порте коммутатора. Например, если VLAN 6, 7 и 8 существуют на AP (беспроводная сеть), то эти VLAN должны быть разрешены на порте коммутатора. Это можно выполнить с помощью команды конфигурации, приведенной ниже:

```
switchport trunk allowed vlan add 6,7,8
```

По умолчанию, порт коммутатора, настраиваемый в качестве магистрали, разрешает прохождение всех VLAN через порт магистрали. [Дополнительные сведения о настройке порта коммутатора см. в документе под названием Взаимодействие с родственными коммутаторами.](#)

Примечание: Разрешение всех VLAN на AP может вызвать проблемы, особенно при работе в больших сетях. Это может привести к чрезмерной загрузке процессора на AP. Во избежание излишней нагрузки на процессор, удалите лишние VLAN на коммутаторе так, чтобы только трафик VLAN, который интересует AP, проходил через AP.

[Точки доступа VLAN](#)

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Сведения о точках доступа VLAN

В этом разделе рассматриваются понятия о том, как развернуть VLAN на точках доступа и обращается к этой схеме сети.

В этом примере сети, VLAN 1 является собственной VLAN, а VLAN 10, 20, 30 и 40 образуют магистраль в другой стойке коммутатора. Только VLAN 10 и 30 преобразованы в беспроводной домен. Собственная VLAN необходима для обеспечения возможностей управления и аутентификации клиентов.

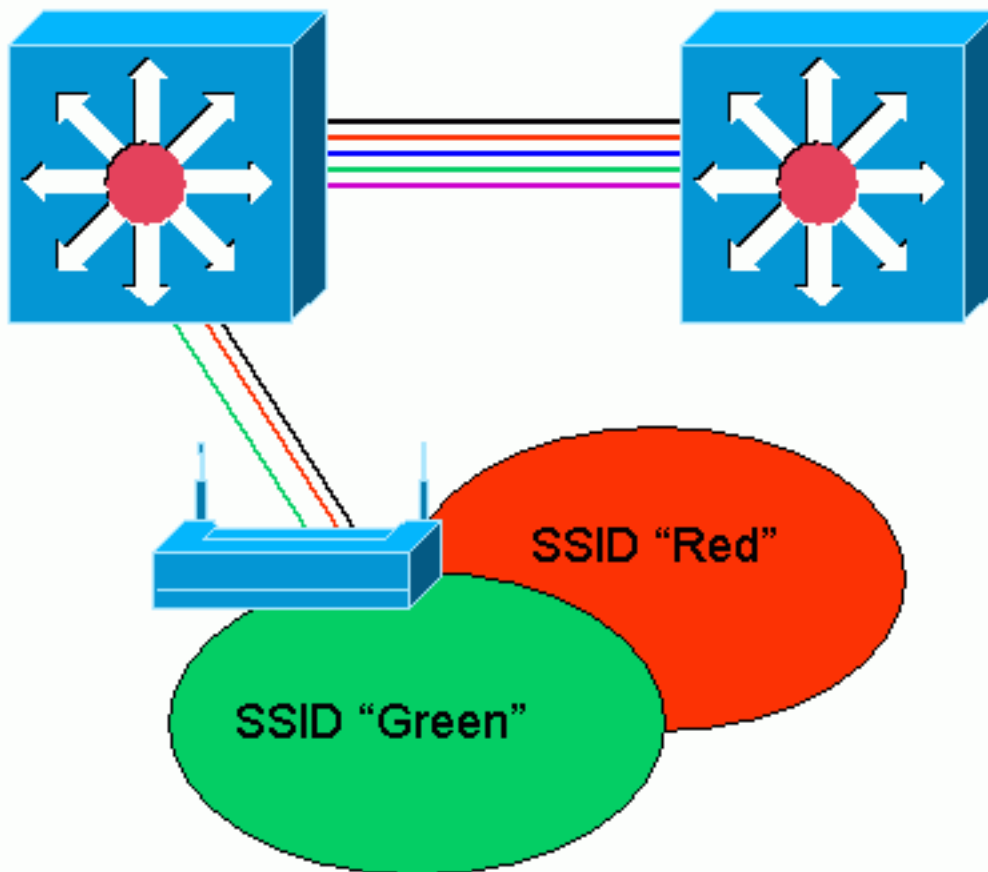
VLAN 1 (Native)

VLAN 10

VLAN 20

VLAN 30

VLAN 40



Настройка точки доступа

Для настройки точки доступа для VLAN выполните эти шаги:

1. От GUI AP нажмите Services> VLAN для навигации к **Сервисам: страница VLAN**. Первый шаг должен настроить собственный VLAN. В меню **Current VLAN List** выберите **New**. Введите номер VLAN собственного VLAN в поле "Идентификатор VLAN". Номер VLAN должен совпадать с Native VLAN, настроенной на коммутаторе. Так как интерфейс BVI 1 связан с субинтерфейсом Native VLAN, то IP-адрес, назначаемый интерфейсу BVI 1, должен принадлежать той же самой IP-подсети, что и другие устройства инфраструктуры сети (это может быть интерфейс SC0 на коммутаторе Catalyst, под управлением операционной системы CatOS.) Для выбора Native VLAN установите флажок. Установите флажки полей для интерфейса радиомодуля или интерфейсов, к которым применяется VLAN. Щелкните "Применить".

The screenshot displays the Cisco 1200 Access Point configuration interface. The main content area is titled "Services: VLAN" and is divided into several sections:

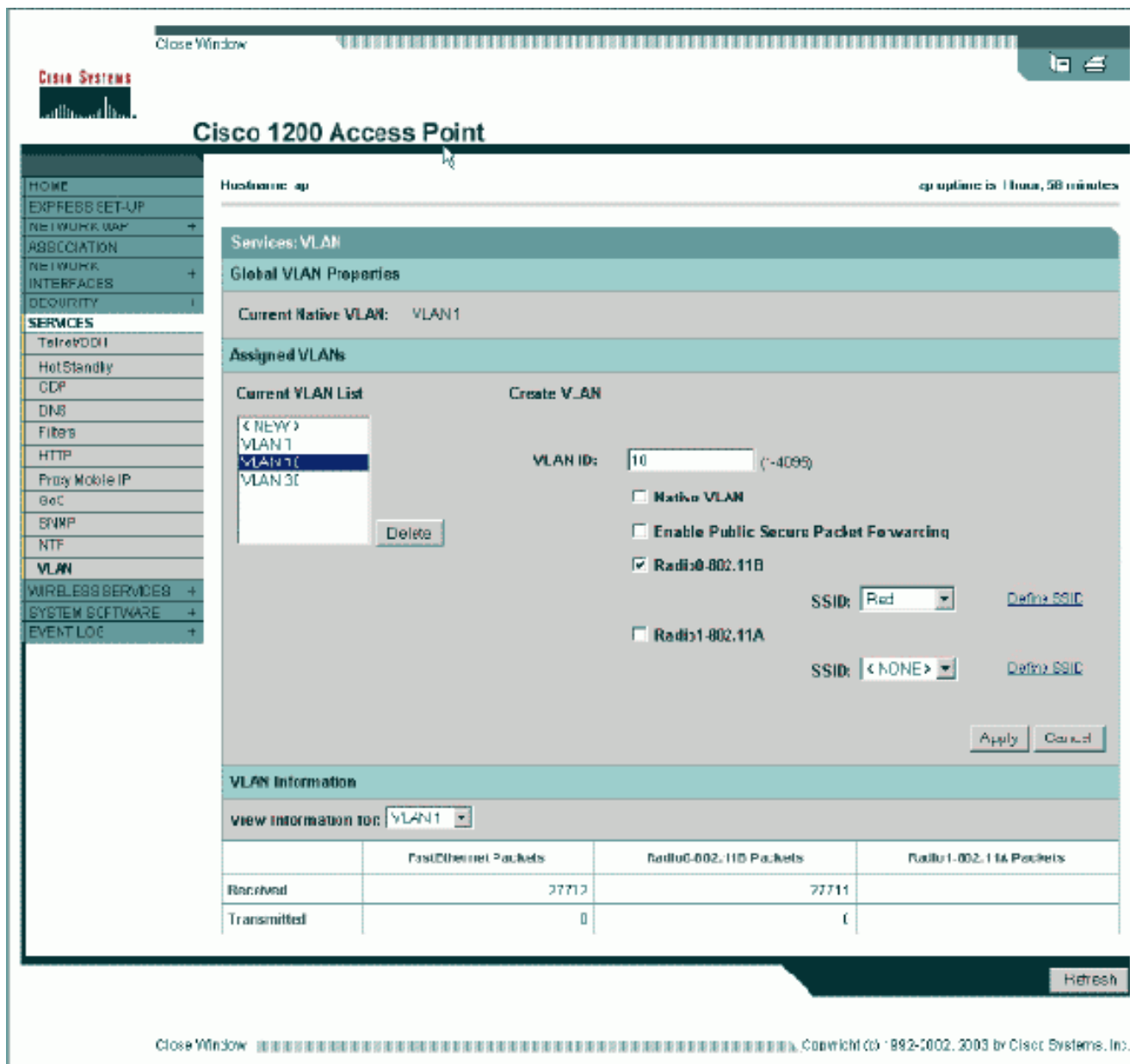
- Global VLAN Properties:** Shows "Current Native VLAN: VLAN1".
- Assigned VLANs:**
 - Current VLAN List:** A list box containing "<NEW>", "VLAN1", "VLAN10", and "VLAN30". A "Delete" button is located below the list.
 - Create VLAN:**
 - VLAN ID:** A text field containing "1" with a range indicator "(1-4095)".
 - Native VLAN**
 - Enable Public Secure Packet Forwarding**
 - Radio0-802.11B** with an "SSID: <NONE>" dropdown and a "Define SSID" link.
 - Radio1-802.11A** with an "SSID: <NONE>" dropdown and a "Define SSID" link.
- VLAN Information:**
 - View information for:** A dropdown menu set to "VLAN1".
 - Table:**

	FastEthernet Packets	Radio0-802.11B Packets	Radio1-802.11A Packets
Received	77712	77711	
Transmitted	0	0	

At the bottom right of the configuration area, there are "Apply" and "Cancel" buttons. Below the configuration area is a "Refresh" button. The footer of the page contains the text "Close Window" and "Copyright © 1992-2002, 2003 by Cisco Systems, Inc."

Или подайте следующие команды из командной строки: AP# `configure terminal` Enter configuration commands, one per line. End with CNTL/Z. AP(config)# `interface Dot11Radio0.1` AP(config-subif)# `encapsulation dot1q 1 native` AP(config-subif)# `interface FastEthernet0.1` AP(config-subif)# `encapsulation dot1q 1 native` AP(config-subif)# `end` AP# `write memory`

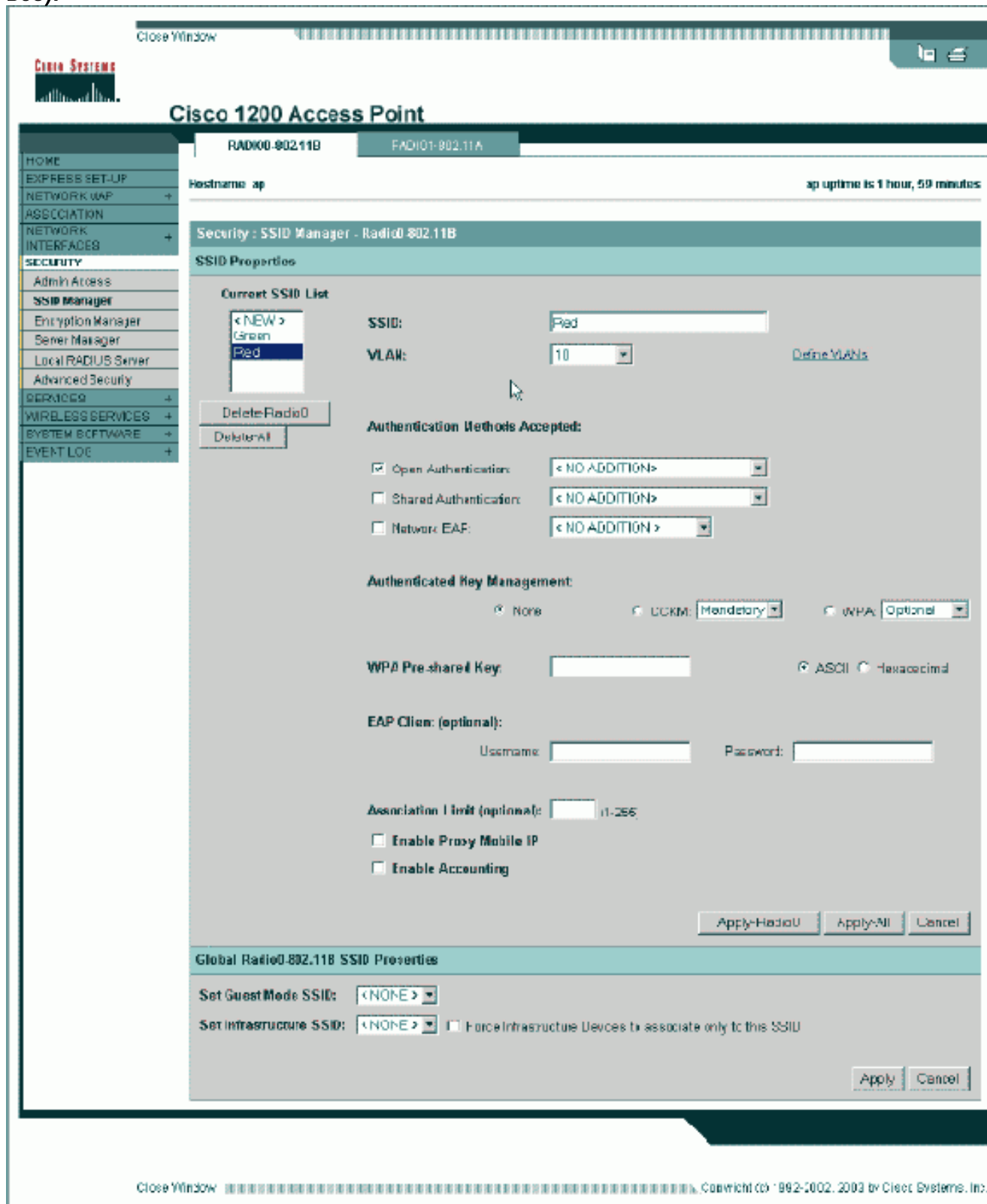
- Для настройки других VLAN выполните эти действия: В меню **Current VLAN List** выберите **New**. В поле "Код VLAN" введите номер нужной виртуальной локальной сети. Номер VLAN должен согласовываться с VLAN, настроенной на коммутаторе. Установите флажки полей для интерфейса радиомодуля или интерфейсов, к которым применяется VLAN. Щелкните **"Применить"**.



Или подайте следующие команды из командной строки: `AP# configure terminal` Enter configuration commands, one per line. End with CNTL/Z. `AP(config)# interface Dot11Radio0.10` `AP(config-subif)# encapsulation dot1q 10` `AP(config-subif)# interface FastEthernet0.10` `AP(config-subif)# encapsulation dot1q 10` `AP(config-subif)# end` `AP# write memory` Повторите действия, описанные в пунктах с 2а по 2д для каждой необходимой VLAN или введите нижеследующие команды в интерфейсе командной строки, изменив необходимым образом номера субинтерфейсов и VLAN: `AP# configure terminal` Enter configuration commands, one per line. End with CNTL/Z. `AP(config)# interface Dot11Radio0.30` `AP(config-subif)# encapsulation dot1q 30` `AP(config-subif)# interface FastEthernet0.30` `AP(config-subif)# encapsulation dot1q 30` `AP(config-subif)# end` `AP# write memory`

- Следующий шаг должен привязать настроенные VLAN к SSIDs. Чтобы сделать это, нажмите **Security> SSID Manager**. **Примечание:** Вы не должны привязывать каждую VLAN, определенную на точке доступа с SSID. Например, по причинам, связанным с обеспечением безопасности, большинство установок точек доступа не связывают SSID с Native VLAN. Для создания нового SSID выберите **New**. В поле SSID введите необходимый SSID (чувствителен к регистру). Выберите из раскрывающегося списка необходимый номер VLAN, которому будет сопоставлен данный SSID. **Примечание:** Для хранения этого документа в его намеченной области безопасность для SSID не обращена. Чтобы создать идентификатор комплекта услуг на выбранном radio, нажмите кнопку **Apply RadioX** (Применить RadioX). Для создания

идентификатора для всех радиоинтерфейсов нажмите кнопку Apply All (Применить все).



Или подайте следующие команды из командной строки: `AP# configure terminal` Enter configuration commands, one per line. End with CNTL/Z. `AP(config)# interface Dot11Radio0` `AP(config-if)# ssid Red` `AP(config-if-ssid)# vlan 10` `AP(config-if-ssid)# end` `AP# write memory`

4. Повторите действия, описанные в пунктах с 3а по 3д для каждого необходимого SSID или введите нижеследующие команды в интерфейсе командной строки, изменив SSID необходимым образом. `AP# configure terminal` Enter configuration commands, one per line. End with CNTL/Z. `AP(config)# interface Dot11Radio0` `AP(config-if)# ssid Green` `AP(config-if-ssid)# vlan 30` `AP(config-if-ssid)# end` `AP# write memory` **Примечание:** Эти примеры не

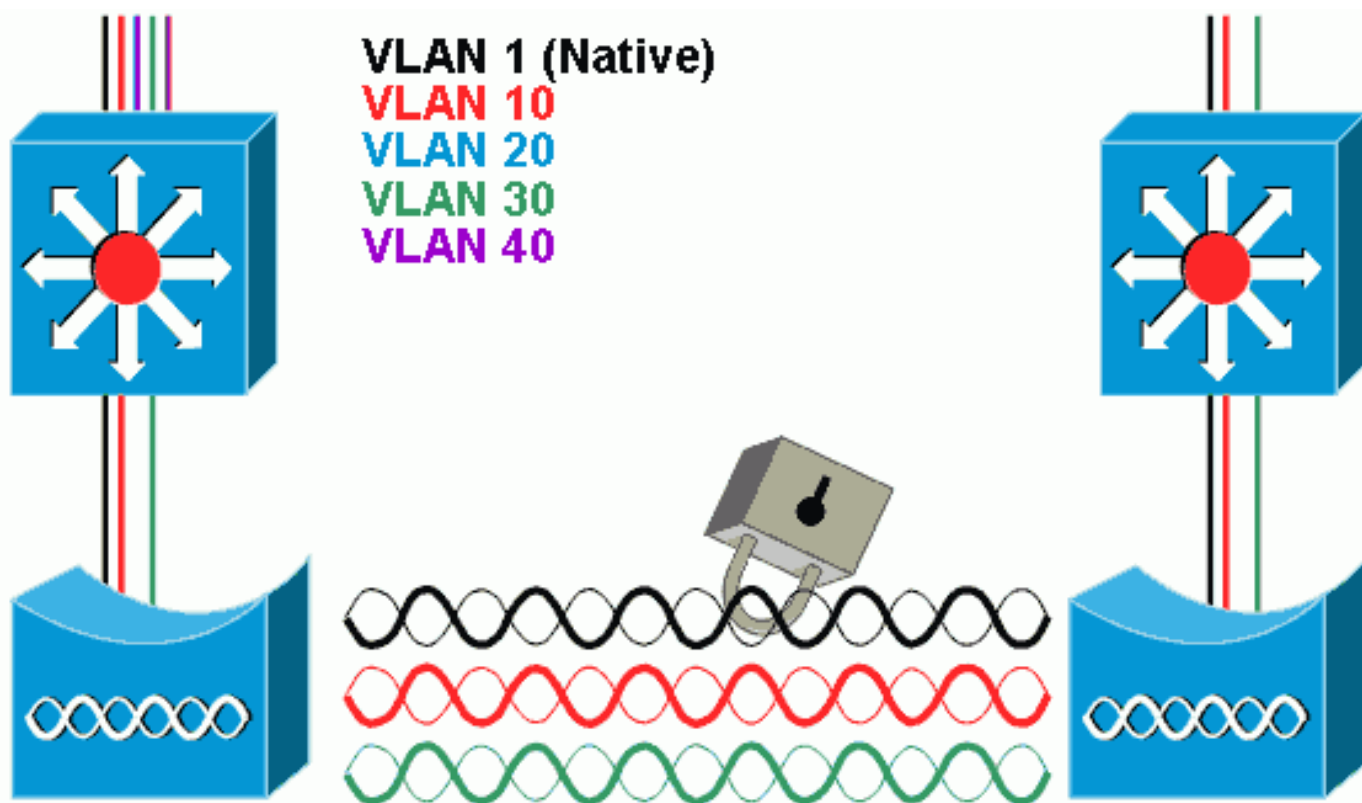
включают аутентификацию. Некоторым клиентам для соединения необходимы ряд форм аутентификации (Open, Network-EAP и т.д.).

VLAN на мостах

Сведения о мостах

В этом разделе рассматриваются понятия, отнесенные к тому, как развернуть VLAN на мостах и обращается к этой схеме сети.

В этом примере сети, VLAN 1 является собственной VLAN, кроме того, существуют VLAN 10, 20, 30 и 40. Только VLAN 10 и 30 расширены на другую сторону канала. Беспроводной канал шифруется.



Для шифрования данных, проходящих по радиоканалу, примените шифрование только к SSID для Native VLAN. Это шифрование применяется ко всем остальным VLAN. При использовании мостов отсутствует необходимость в связывании отдельного SSID с каждой VLAN. Настройки VLAN одинаковы как для корневых, так и для некорневых мостов.

Настройка моста

Для настройки моста для VLAN, как пример схемы сети, выполните эти шаги:

1. От GUI AP нажмите **Services> VLAN** для навигации к **Сервисам: страница VLAN**. Первый шаг должен настроить Собственный VLAN. Чтобы сделать это, выберите **<New>** из Текущего СПИСКА VLAN. Введите номер VLAN собственного VLAN в поле "Идентификатор VLAN". Номер VLAN должен согласовываться с Native VLAN, настроенной на коммутаторе. Так как интерфейс BVI 1 связан с субинтерфейсом Native

VLAN, то IP-адрес, назначаемый интерфейсу VVI 1 , должен принадлежать той же самой IP-подсети, что и другие устройства инфраструктуры сети (это может быть интерфейс SC0 на коммутаторе Catalyst, под управлением операционной системы CatOS.) Для выбора Native VLAN установите флажок.Щелкните "Применить".

The screenshot shows the Cisco 1200 Access Point configuration page. The left sidebar contains a navigation menu with categories like HOME, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Services: VLAN" and includes sections for "Global VLAN Properties", "Assigned VLANs", and "VLAN Information".

Global VLAN Properties: Current Native VLAN: VLAN1

Assigned VLANs: A table with columns "Current VLAN List" and "Create VLAN". The "Current VLAN List" contains entries: <NEW>, VLAN1 (selected), VLAN1C, and VLAN3C. A "Delete" button is present below the list.

Create VLAN: VLAN ID: 1 (-4095). Checkboxes: Native VLAN, Enable Public Secure Packet Forwarding, Radio0-802.11B, Radio1-802.11A. SSID fields are set to <NONE> with "Define SSID" links.

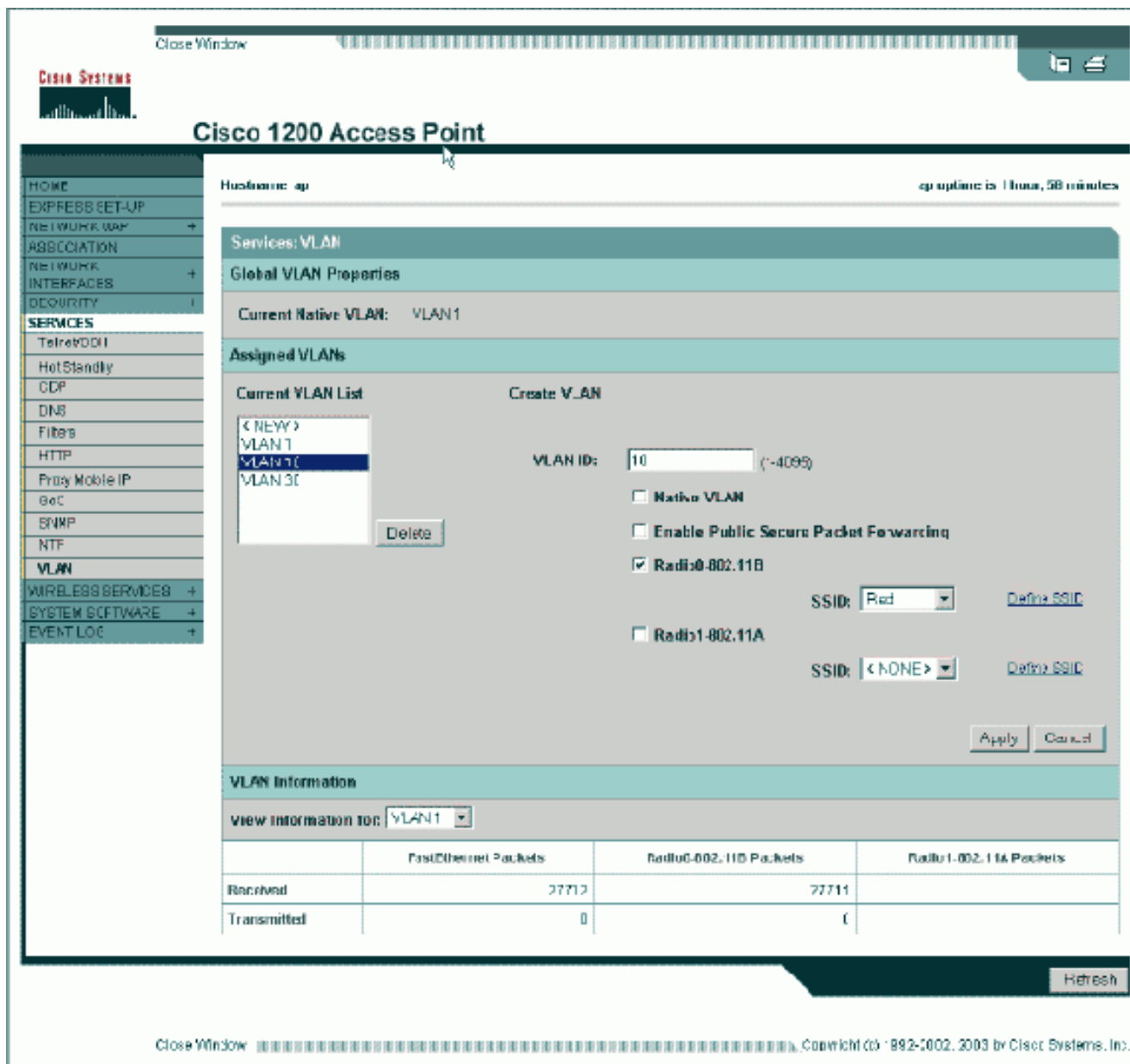
VLAN Information: View information for: VLAN1. A table shows packet statistics:

	FastEthernet Packets	Radio0-802.11B Packets	Radio1-802.11A Packets
Received	27712	77711	
Transmitted	0		

Buttons "Apply" and "Cancel" are at the bottom right of the configuration area. A "Refresh" button is at the bottom right of the page. The footer contains "Copyright © 1992-2002, 2003 by Cisco Systems, Inc."

Или подайте следующие команды из командной строки:bridge# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. bridge(config)# **interface Dot11Radio0.1** bridge(config-subif)# **encapsulation dot1Q 1 native** bridge(config-subif)# **interface FastEthernet0.1** bridge(config-subif)# **encapsulation dot1Q 1 native** bridge(config-subif)# **end** bridge# **write memory**

- Для настройки других VLAN выполните эти действия:В меню **Current VLAN List** выберите **New**.В поле "Код VLAN" введите номер нужной виртуальной локальной сети. Номер VLAN должен согласовываться с VLAN, настроенной на коммутаторе.Щелкните "Применить".



Или подайте следующие команды из командной строки: `bridge# configure terminal` Enter configuration commands, one per line. End with CNTL/Z. `bridge(config)# interface Dot11Radio0.10` `bridge(config-subif)# encapsulation dot1q 10` `bridge(config-subif)# interface FastEthernet0.10` `bridge(config-subif)# encapsulation dot1q 10` `bridge(config-subif)# end` `bridge# write memory` Повторите действия, описанные в пунктах с 2а по 2с для каждой необходимой VLAN или введите нижеследующие команды в интерфейсе командной строки, изменив необходимым образом номера субинтерфейсов и VLAN. `AP# configure terminal` Enter configuration commands, one per line. End with CNTL/Z. `bridge(config)# interface Dot11Radio0.30` `bridge(config-subif)# encapsulation dot1q 30` `bridge(config-subif)# interface FastEthernet0.30` `bridge(config-subif)# encapsulation dot1q 30` `bridge(config-subif)# end` `bridge# write memory`

- От Диспетчера SSID (под элементом меню **Security > SSID Manager**) привязывают Собственный VLAN к SSID. **Примечание:** Когда вы соединяете, единственный SSID, который необходимо привязать к VLAN, является тем, который коррелирует к Собственному VLAN. Этот SSID следует определить как SSID инфраструктуры. В меню **Current SSID List** выберите **New**. В поле SSID введите необходимый SSID (чувствителен к регистру). Выберите из выпадающего списка необходимый номер VLAN, который коррелирует с Native VLAN. **Примечание:** Для хранения этого документа в его намеченной области безопасность для SSID не обращена. Нажмите кнопку **Apply** для того, чтобы создать SSID на радиомодуле и связать его с собственной

VLAN.

The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "labbr1310ip93" and the uptime is "3 days, 18 hours, 45 minutes".

The left sidebar contains a navigation menu with the following items: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (expanded), Admin Access, Encryption Manager, SSID Manager (selected), Server Manager, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.

The main content area is titled "Security: SSID Manager". It contains the following sections:

- SSID Properties**
 - Current SSID List**: A table with one entry: "< NEW >". A "Delete" button is located below the table.
 - SSID**: A text input field containing "Black".
 - VLAN**: A dropdown menu set to "1" with a "Define VLANs" link next to it.
 - Network ID**: A text input field containing "0-4096".
- Authentication Settings**
 - Authentication Methods Accepted**:
 - Open Authentication: < NO ADDITION >
 - Shared Authentication: < NO ADDITION >
 - Network EAP: < NO ADDITION >
 - Server Priorities**:
 - EAP Authentication Servers
 - MAC Authentication Servers

Прокрутите вниз назад к концу страницы, и под Глобальным SSID Radio0-802.11G Свойства выбирают SSID из выпадающего списка Set Infrastructure SSID. Щелкните "Применить".

The screenshot shows the "Global Radio0-802.11G SSID Properties" configuration page. It contains the following fields and options:

- Username**: A text input field.
- Password**: A text input field.
- Apply** and **Cancel** buttons.
- Global Radio0-802.11G SSID Properties** section:
 - Set Guest Mode SSID**: A dropdown menu set to "< NONE >".
 - Set Infrastructure SSID**: A dropdown menu set to "Black".
 - Force Infrastructure Devices to associate only to this SSID.
- Apply** and **Cancel** buttons.

Или подайте следующие команды из командной строки: AP# `configure terminal` Enter configuration commands, one per line. End with CNTL/Z. AP(config)# `interface Dot11Radio0` AP(config-if)# `ssid Black` AP(config-if-ssid)# `vlan 1` AP(config-if-ssid)# `infrastructure-ssid` AP(config-if-ssid)# `end` AP# `write memory` **Примечание:** Когда VLAN используются, SSIDs настроены под физическим интерфейсом Dot11Radio, не под любым локальным подчиненным интерфейс. **Примечание:** Данный пример не включает аутентификацию.

Корневые и некорневые мосты для соединения требуют ряда форм аутентификации (Open, Network-EAP и т.д.).

[Используйте сервер RADIUS для присвоения пользователей на VLAN](#)

Можно настроить Сервер проверки подлинности RADIUS для присвоения пользователей или групп пользователей к определенной VLAN, когда они аутентифицируются на сети. Для получения информации об этой функции обратитесь к разделу [Использование сервера RADIUS Назначить Пользователей на VLAN](#) руководства по настройке ПО Cisco IOS документа для точек доступа Cisco Aironet, 12.4 (3-граммовых) JA и 12.3 (8) JEB.

[Используйте сервер RADIUS для динамического присвоения группы мобильности](#)

Можно также настроить сервер RADIUS для динамического присвоения групп мобильности на пользователей или группы пользователей. Это избавляет от необходимости настраивать множественный SSIDs на точке доступа. Вместо этого необходимо настроить только один SSID на точку доступа. Для получения информации об этой функции обратитесь к разделу [Использование сервера RADIUS для Динамического Присвоения Группы мобильности](#) руководства по настройке ПО Cisco IOS документа для точек доступа Cisco Aironet, 12.4 (3-граммовых) JA и 12.3 (8) JEB.

[Конфигурация группы мостов на точках доступа и мостах](#)

В целом мостовые группы создают сегментированные переключающиеся домены. Трафик ограничен хостами в каждой группе мостов, но не между мостовыми группами. Коммутатор передает трафик только среди хостов, которые составляют группу мостов, которая ограничивает широковещание и многоадресный трафик (затопление) к только тем хостам. Мостовые группы уменьшают перегрузку сети и предоставляют дополнительную сетевую безопасность, когда они сегментируют трафик в определенные области сети.

См. [Мостовое соединение Обзора](#) для получения дальнейшей информации.

В беспроводной сети мостовые группы настроены на точках беспроводного доступа и мостах для трафика данных VLAN, которая будет передана от беспроводных сред до проводной стороны и наоборот.

Выполните этот шаг от CLI AP для включения мостовых групп глобально на точке доступа / мост.

Данный пример использует номер группы мостов 1.

AP (настраивает) `#bridge 1`

Примечание: Можно перечислить мостовые группы от 1 до 255.

Настройте радиointерфейс и Интерфейс Fast Ethernet беспроводного устройства, чтобы быть в той же группе мостов. Это создает путь между этими двумя другими интерфейсами, и они находятся в той же VLAN для маркировки целей. В результате данные, переданные с беспроводной стороны до радиointерфейса, переданы к Интерфейсу Ethernet, с которым проводная сеть связана и наоборот. Другими словами, радио и Интерфейсы Ethernet,

которые принадлежат той же группе мостов фактически, соединяют данные между ними.

В точке доступа / мост, у вас должна быть одна группа мостов на VLAN так, чтобы трафик мог пройти от провода до радио и наоборот. Чем больше VLAN, которую вы имеете, который должен передать трафик через радио, тем большие мостовые группы, которые необходимы.

Например, если у вас есть только одна VLAN для передачи трафика через радио проводной стороне сети, настройте только одну группу мостов от CLI AP/моста. Если у вас есть несколько интерфейсов VLAN для передачи трафика от радио до проводной стороны и наоборот, настройте мостовые группы для каждой VLAN в радио-подчиненном интерфейсе, а также подчиненном интерфейсе Fast Ethernet.

1. Настройте группу мостов в беспроводном интерфейсе с **группой мостов dot11radio** интерфейсная команда. Ниже представлен пример.
AP# `configure terminal` Enter configuration commands, one per line. End with CNTL/Z. AP(config)# `interface Dot11Radio0.1`
Ap(config-subif)# `encapsulation dot1q 1 native` Ap(config-subif)# `bridge group 1 !--- Here "1" represents the bridge group number.` ap(config-subif)# `exit`
2. Настройте группу мостов с тем же номером группы моста ("1" в данном примере) в Интерфейсе Fast Ethernet так, чтобы трафик VLAN 1 передали через беспроводной интерфейс этой проводной стороне и наоборот.
Ap(config)# `interface fastEthernet0.1`
Ap(config-subif)# `encapsulation dot1q 1 native` Ap(config-subif)# `bridge group 1 !--- Here "1" represents the bridge group number.` Ap(config-subif)# `exit`
Примечание: При настройке группы мостов на радиоинтерфейсе эти команды установлены автоматически.
`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`
Примечание: При настройке группы мостов на Интерфейсе Fast Ethernet эти команды установлены автоматически.
`no bridge-group 1 source-learning`
`bridge-group 1 spanning-disabled`

[Concurrent Routing and Bridging \(IRB\)](#)

Интегрированная маршрутизация и соединение при помощи мостов позволяет направить определенный протокол между маршрутизируемыми интерфейсами и мостовыми группами, или направить определенный протокол между мостовыми группами. В то время как маршрутизуемый трафик может маршрутизироваться к другим маршрутизируемым интерфейсам или мостовым группам, локальный или немаршрутизируемый трафик может быть соединен среди мостовых интерфейсов в той же группе мостов

С интегрированной маршрутизацией и соединением при помощи мостов можно сделать это:

- Пакеты коммутатора от мостового интерфейса до маршрутизируемого интерфейса
- Пакеты коммутатора от маршрутизируемого интерфейса до мостового интерфейса
- Пакеты коммутатора в той же группе мостов

Включите IRB на точках беспроводного доступа и мостах для маршрутизации трафика между мостовыми группами или между маршрутизируемыми интерфейсами и мостовыми группами. Вам нужны внешний маршрутизатор или Коммутатор 3 уровня для маршрутизации между мостовыми группами или между мостовыми группами и маршрутизируемыми интерфейсами.

Выполните эту команду для включения IRB в AP/мосте.

AP (настраивает) #bridge irb

Интегрированная маршрутизация и соединение при помощи мостов использует понятие Виртуального интерфейса мостовой группы (BVI) для маршрутизации трафика между маршрутизируемыми интерфейсами и мостовыми группами или между мостовыми группами.

BVI является виртуальным интерфейсом в маршрутизаторе Коммутатора 3 уровня, который действует как обычный маршрутизируемый интерфейс. BVI не поддерживает мостовое соединение, но фактически представляет соответствующую группу мостов маршрутизируемым интерфейсам в маршрутизаторе Коммутатора 3 уровня. Это имеет все атрибуты сетевого уровня (такие как адрес сетевого уровня и фильтры), которые применяются к соответствующей группе мостов. Номер интерфейса, назначенный на этот виртуальный интерфейс, соответствует группе мостов, которую представляет этот виртуальный интерфейс. Этот номер является ссылкой между виртуальным интерфейсом и группой мостов.

Выполните эти шаги для настройки BVI на точках доступа и мостах.

1. Настройте BVI и назначьте соответствующее количество группы мостов к BVI. Данный пример назначает номер группы моста 1 на BVI.

```
Ap(configure)#interface BVI 1 Ap(config-if)#ip address 10.1.1.1 255.255.0.0 !--- Assign an IP address to the BVI. Ap(config-if)#no shut
```
2. Позвольте BVI принять и направить пакеты с возможностью трассировки, полученные от его соответствующей группы мостов.

```
Ap(config)# bridge 1 route ip!--- !--- This example enables the BVI to accept and route the IP packet.
```

 Важно понять, что вам только нужен BVI для управления/собственного VLAN, в котором AP расположен (в данном примере, VLAN 1). Вам не нужен BVI ни для какого другого подинтерфейса, независимо от того, сколько VLAN и мостовых групп вы настраиваете на своем AP/мосте. Это вызвано тем, что вы помечаете трафик во всех других VLAN (кроме собственного VLAN) и отправляете его в коммутатор, хотя dot1q соединил интерфейс магистралью на проводную сторону. Например, если у вас есть 2 VLAN в вашей сети, вам нужны две мостовых группы, но только один корреспондент BVI к VLAN управления достаточен в вашей беспроводной сети. Когда вы позволяете направить для данного протокола на виртуальном интерфейсе группы мостовой передачи, пакеты, которые прибывают из маршрутизируемого интерфейса, но предназначены для хоста в соединенном мостом домене, маршрутизируются к виртуальному интерфейсу группы мостовой передачи и переданы соответствующему мостовому интерфейсу. Весь трафик, который маршрутизируется к виртуальному интерфейсу группы мостовой передачи, передан к соответствующей группе мостов как проходящий через мост трафик. Весь маршрутизуемый трафик, полученный на мостовом интерфейсе, маршрутизируется к другим маршрутизируемым интерфейсам, как будто он прибывает непосредственно из виртуального интерфейса группы мостовой передачи. См. [Настраивают Мостовое соединение](#) для более подробной информации о мостовом соединении и IRB.

[Взаимодействие с родственными коммутаторами](#)

В этом разделе приводятся сведения о настройке или о проверке настройки коммутаторов Cisco, подключенных к беспроводному оборудованию Cisco Aironet.

Примечание: [Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд \(только для зарегистрированных клиентов\).](#)

[Конфигурация коммутатора—ОС Catalyst](#)

Для настройки коммутатора, который выполняет Catalyst OS для транкинга VLAN к точке доступа, синтаксис команды является **set trunk <модуль #/порт #> на dot1q** и **set trunk <модуль #/порт #> <список vlan>**.

Для схемы сети из примера эти команды будут иметь следующий синтаксис:

```
set trunk 2/1 on dot1q set trunk 2/1 1,10,30
```

[Настройка коммутатора — Коммутаторы Catalyst на основе операционной системы IOS](#)

От режима конфигурации интерфейса введите эти команды, если вы хотите:

- Настройте порт коммутатора для транкинга VLAN к точке доступа
- На Коммутаторе Catalyst, который выполняет IOS
- CatIOS включает, но не ограничен:6x004x0035x0295x

```
switchport mode trunk switchport trunk encapsulation dot1q switchport nonegotiate switchport trunk native vlan 1 switchport trunk allowed vlan add 1,10,30
```

Примечание: IOS базировался, беспроводное оборудование Cisco Aironet не поддерживает Протокол DTP, таким образом, коммутатор не должен пытаться выполнить согласование о нем.

[Настройка коммутатора в ТЪ Catalyst 2900XL/3500XL](#)

От режима конфигурации интерфейса введите эти команды, если вы хотите настроить порт коммутатора для транкинга VLAN к точке доступа на Catalyst 2900XL или 3500XL коммутатор, который выполняет IOS:

```
switchport mode trunk switchport trunk encapsulation dot1q switchport trunk native vlan 1 switchport trunk allowed vlan 1,10,30
```

[Проверка](#)

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Проверка беспроводного оборудования](#)

- **show vlan** все VLAN, в настоящее время настраиваемые на точке доступа и их

```
STATUS#show vlan Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation) vLAN Trunk Interfaces:
FastEthernet0.1 Dot11Radio0.1 Virtual-Dot11Radio0.1 This is configured as native Vlan for
the following interface(s) : FastEthernet0 Dot11Radio0 Virtual-Dot11Radio0 Protocols
Configured: Address: Received: Transmitted: Bridging Bridge Group 1 36954 0 Bridging Bridge
Group 1 36954 0 Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation) vLAN Trunk Interfaces:
FastEthernet0.10 Dot11Radio0.10 Virtual-Dot11Radio0.10 Protocols Configured: Address:
```

```
Received: Transmitted: Bridging Bridge Group 10 5297 0 Bridging Bridge Group 10 5297 0
Bridging Bridge Group 10 5297 0 Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation) vLAN Trunk
Interfaces: FastEthernet0.30 Dot11Radio0.30 Virtual-Dot11Radio0.30 Protocols Configured:
Address: Received: Transmitted: Bridging Bridge Group 30 5290 0 Bridging Bridge Group 30
5290 0 Bridging Bridge Group 30 5290 0 ap#
```

- **show dot11 associations в ТЪ** отображает сведения о связанных клиентах для каждого SSID/VLAN
ap#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [Green] :
SSID [Red] : Others: (not related to any ssid) ap#

[Проверить коммутатор](#)

- На коммутаторе на основе Catalyst OS **show trunk <модуль #/порт #>** — отображает статус транка на данном порту
Console> (enable) show trunk 2/1
* - indicates vtp domain mismatch
Port Mode Encapsulation Status Native vlan

2/1 on dot1q trunking 1 Port Vlans allowed on trunk -----
----- 2/1 1,10,30 Port Vlans allowed and active in management
domain ----- 2/1 1,10,30
Port Vlans in spanning tree forwarding state and not pruned -----
----- 2/1 1,10,30 Console> (enable)
- На коммутаторе на основе IOS **fastEthernet show interface <модуль #/порт #> транк** — отображает статус транка на данном интерфейсе
2950g#show interface fastEthernet 0/22 trunk

Port Mode Encapsulation Status Native vlan
Fa0/22 on 802.1q trunking 1 Port Vlans allowed on trunk **Fa0/22 1,10,30** Port Vlans allowed
and active in management domain Fa0/22 1,10,30 Port Vlans in spanning tree forwarding state
and not pruned Fa0/22 1,10,30 2950gA#
- На Коммутаторе Catalyst 2900XL **fastEthernet show interface <модуль #/порт #> порт коммутатора** — отображает статус транка на данном интерфейсе
cat3524xl#show interface fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk Administrative Trunking Encapsulation: dot1q **Operational Trunking**
Encapsulation: dot1q Negotiation of Trunking: Disabled Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default) **Trunking VLANs Enabled: 1,10,30,1002-1005** **Trunking**
VLANs Active: 1,10,30 Pruning VLANs Enabled: 2-1001 Priority for untagged frames: 0 Override
vlan tag priority: FALSE Voice VLAN: none Appliance trust: none Self Loopback: No wlan-
cat3524xl-a#

[Устранение неполадок](#)

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

[Дополнительные сведения](#)

- [Конфигурация сетей VLAN \(Руководство по конфигурированию точек доступа\)](#)
- [VLAN Настройки \(руководство конфигурации моста\)](#)
- [Техническая поддержка группирования магистралей](#)
- [Взаимодействие с родственными коммутаторами](#)
- [Страница поддержки технологии магистрального соединения](#)
- [Обзор мостового соединения](#)

- [Пример настройки типов аутентификации беспроводной связи на фиксированном ISR](#)
- [Пример настройки типов аутентификации на фиксированном ISR с помощью SDM](#)
- [Пример конфигурации подключения к беспроводной локальной сети с использованием маршрутизатора ISR с WEP-шифрованием и LEAP-аутентификацией](#)
- [Пример конфигурации базового беспроводного подключения LAN](#)
- [Cisco Systems – техническая поддержка и документация](#)