

# Настройте ASA 5506W-X с IP на по умолчанию или конфигурацией несколько интерфейсов VLAN

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Сетевые графики](#)

[Настройка](#)

[Шаг 1. Модифицируйте Интерфейсный IP - конфигурацию на ASA](#)

[Шаг 2. Модифицируйте параметры настройки пула DHCP и на внутри и на интерфейсы Wi-Fi](#)

[Шаг 3. Задайте сервер DNS для передачи клиентам DHCP WiFi и внутренней части](#)

[Шаг 4. . Модифицируйте конфигурацию доступа HTTP на ASA для доступа Менеджера устройств адаптивной безопасности \(ASDM\) \(ASDM\):](#)

[Шаг 5. . Модифицируйте Интерфейсного IP для менеджмента точки доступа в консоли WLAN \(интерфейсный BVI1\):](#)

[Шаг 6. Модифицируйте default-gateway на WAP](#)

[Шаг 7. Модифицируйте управление IP-адресами модуля FirePOWER \(Необязательно\)](#)

[Если интерфейс ASA Management1/1 связан с внутренним коммутатором:](#)

[Если ASA HE связан с внутренним коммутатором:](#)

[Шаг 8. Соединитесь с GUI AP, чтобы включить радио и установить другую конфигурацию WAP](#)

[Конфигурация интерфейса командой строки WAP для одиночной беспроводной сети VLAN с помощью модифицировала диапазоны IP](#)

[Конфигурации](#)

[Конфигурация ASA](#)

[Aironet Конфигурация WAP \(без config SSID в качестве примера\)](#)

[Конфигурация модуля FirePOWER \(с внутренним коммутатором\)](#)

[Конфигурация модуля FirePOWER \(без внутреннего коммутатора\)](#)

[Проверка](#)

[Настройте DHCP со множественными беспроводными сетями VLAN](#)

[Шаг 1. Удалите Существующую конфигурацию DHCP на Gig1/9](#)

[Шаг 2. Создайте подинтерфейсы для каждой VLAN на Gig1/9](#)

[Шаг 3. Определяйте пул DHCP для каждой VLAN](#)

[Шаг 4. . Настройте точку доступа SSIDs, сохраните config и перезагрузите модуль](#)

[Устранение неполадок](#)

## Введение

Этот документ описывает, как выполнить начальную установку и конфигурацию устройства

адаптивной защиты Cisco (ASA) устройство 5506W-X, когда схема адресации IP по умолчанию должна модифицироваться для вписывания в существующую сеть или если требуются множественные беспроводные сети VLAN. Существует несколько изменений конфигурации, которые требуются при изменении IP - адресов по умолчанию, чтобы обратиться к точке беспроводного доступа (WAP), а также гарантировать, что другие сервисы (такие как DHCP) продолжают функционировать как ожидалось. Кроме того, этот документ предоставляет некоторые примеры конфигурации интерфейса командой строки для интегрированной Точки беспроводного доступа (WAP), чтобы упростить завершить начальную конфигурацию WAP. Этот документ предназначен для добавления существующего Cisco ASA 5506-X Краткое руководство по началу работы, доступное на [Web - сайте Cisco](#).

## Предварительные условия

Этот документ только применяется к начальной конфигурации устройства Cisco ASA5506W-X, которое содержит точку беспроводного доступа и только предназначено для адресации к различным изменениям, необходимым, когда вы модифицируете существующую схему IP-адресации или добавляете дополнительные беспроводные сети VLAN. Для установок конфигурации по умолчанию существующий [ASA](#) нужно сослаться [на 5506-X Краткое руководство по началу работы](#).

## Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Устройство Cisco ASA 5506W-X
- Клиентский компьютер с программой эмуляции терминала, такой как Шпаклевка, SecureCRT, и т.д.
- Консольный кабель и последовательный адаптер терминала ПК (DB-9 к RJ-45)

## Используемые компоненты

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

- Устройство Cisco ASA 5506W-X
- Клиентский компьютер с программой эмуляции терминала, такой как Шпаклевка, SecureCRT, и т.д.
- Консольный кабель и последовательный адаптер терминала ПК (DB-9 к RJ-45)
- Модуль ASA FirePOWER
- Интегрированный Cisco Aironet 702i точка беспроводного доступа (Встроенный WAP)

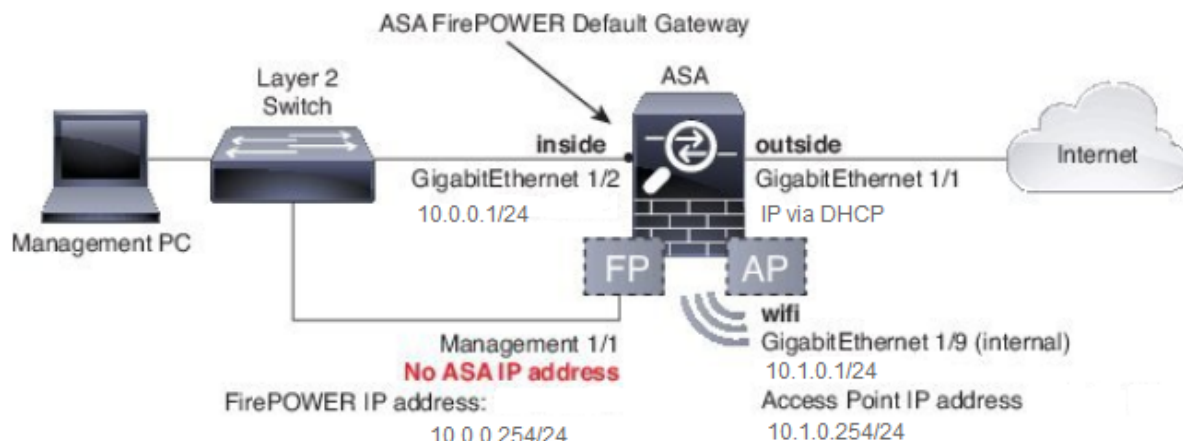
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Сетевые графики

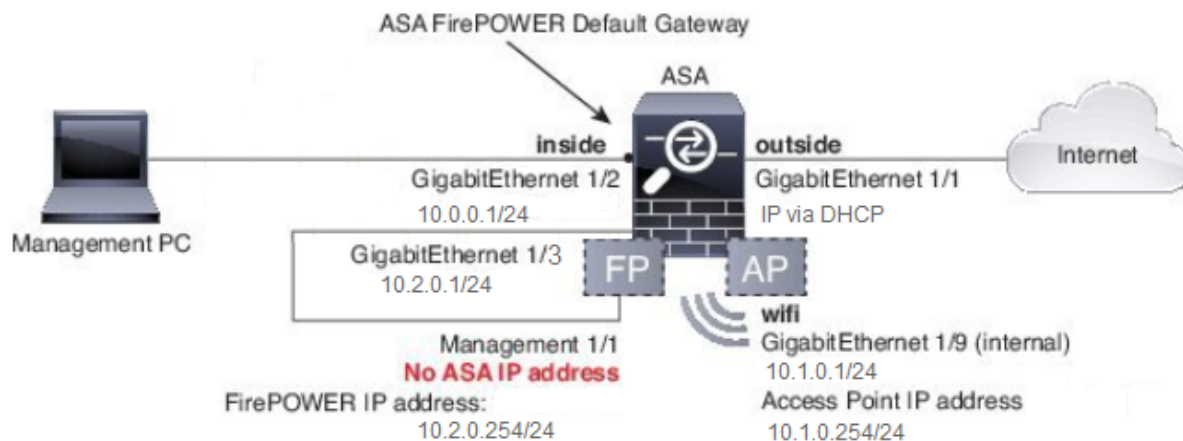
Как показано в этом образе, примерах IP-адресации, которая будет применена в двух

другой топологии:

### ASA + FirePOWER с внутренним коммутатором:



### ASA + FirePOWER без внутреннего коммутатора:



## Настройка

Эти шаги должны быть выполнены в заказе после того, как вы включите и загрузите ASA с консольным кабелем, связанным с клиентом.

### Шаг 1. Модифицируйте Интерфейсный IP - конфигурацию на ASA

Настройте внутреннее (GigabitEthernet 1/2) и Wi-Fi (GigabitEthernet 1/9) интерфейсы для имени IP-адресов по мере необходимости в существующей среде. В данном примере внутренние клиенты находятся в 10.0.0.1/24 сети, и клиенты WIFI находятся в 10.1.0.1/24 сети.

```
asa(config)# interface gigabitEthernet 1/2
asa(config-if)# ip address 10.0.0.1 255.255.255.0
```

```
asa(config)# interface gigabitEthernet 1/9
```

```
asa(config-if)# ip address 10.1.0.1 255.255.255.0
```

**Примечание:** Вы получите это предупреждение при изменении вышеупомянутых IP-адресов интерфейса. Это ожидается.

```
Interface address is not on same subnet as DHCP pool  
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed
```

## Шаг 2. Модифицируйте параметры настройки пула DHCP и на внутри и на интерфейсы Wi-Fi

Если ASA должен использоваться в качестве сервера DHCP в среде, этот шаг требуется. Если другой сервер DHCP используется для присвоения IP-адресов на клиентов тогда, DHCP должен быть отключен на ASA в целом. Так как вы теперь изменили нашу схему IP-адресации, необходимо изменить существующие Диапазоны IP-адресов, которые ASA предоставляет клиентам. Эти команды создадут новые пулы для соответствия с диапазоном нового IP-адреса:

```
asa(config)# dhcpd address 10.0.0.2-10.0.0.100 inside  
asa(config)# dhcpd address 10.1.0.2-10.1.0.100 wifi
```

Также модификация пулов DHCP отключит предыдущий сервер DHCP на ASA, и необходимо будет реактивировать его.

```
asa(config)# dhcpd enable inside
```

```
asa(config)# dhcpd enable wifi
```

Если вы не измените IP-адреса интерфейса прежде, чем внести изменения DHCP тогда, то вы получите эту ошибку:

```
asa(config)# dhcpd address 10.0.0.2-10.0.0.100 inside  
Address range subnet 10.0.0.2 or 10.0.0.100 is not the same as inside interface subnet  
192.168.1.1
```

## Шаг 3. Задайте сервер DNS для передачи клиентам DHCP WiFi и внутренней части

Когда они назначают IP-адреса через DHCP, большинству клиентов также должен назначить сервер DNS сервер DHCP. Эти команды настроят ASA для включения сервера DNS, расположенного в 10.0.0.250 всем клиентам. Необходимо заменить 10.0.0.250 или внутренний сервер DNS или сервер DNS, предоставленный интернет-провайдером.

```
asa(config)# dhcpd dns 10.0.0.250 interface inside  
asa(config)# dhcpd dns 10.0.0.250 interface wifi
```

## Шаг 4. . Модифицируйте конфигурацию доступа HTTP на ASA для доступа Менеджера устройств адаптивной безопасности (ASDM) (ASDM):

Так как IP-адресация была изменена, доступ HTTP к ASA также должен модифицироваться так, чтобы клиенты на внутренней части и сетях WiFi могли обратиться к ASDM для управления ASA.

```
asa(config)# no http 192.168.1.0 255.255.255.0 inside
```

```
asa(config)# no http 192.168.10.0 255.255.255.0 wifi
asa(config)# http 0.0.0.0 0.0.0.0 inside asa(config)# http 0.0.0.0 0.0.0.0 wifi
```

**Примечание:** Эта конфигурация позволяет любому клиенту на внутренней части или интерфейсах Wi-Fi обращаться к ASA через ASDM. Как оптимальный метод безопасности, необходимо ограничить область адресов доверяемым клиентам только.

## Шаг 5. . Модифицируйте Интерфейсного IP для менеджмента точки доступа в консоли WLAN (интерфейсный BVI1):

```
asa# session wlan console
ap>enable
Password: Cisco
ap#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#interface BVI1
ap(config-if)#ip address 10.1.0.254 255.255.255.0
```

## Шаг 6. Модифицируйте default-gateway на WAP

Этот шаг требуется так, чтобы WAP знал, куда передать весь трафик, который не инициируется на локальной подсети. Это требуется, чтобы предоставлять для доступа к GUI WAP через HTTP от клиента на Внутреннем интерфейсе ASA.

```
ap(config)#ip default-gateway 10.1.0.1
```

## Шаг 7. Модифицируйте управление IP-адресами модуля FirePOWER (Необязательно)

Если вы также планируете развернуть Cisco FirePOWER (также известный как SFR) модуль тогда, также необходимо изменить его IP-адрес для доступа, это от физического Management1/1 взаимодействует на ASA. Существует два основных сценария развертывания, которые определяют, как настроить ASA и модуль SFR:

1. Топология, в которой интерфейс ASA Management1/1 связан с внутренним коммутатором (согласно обычному Краткому руководству по началу работы)
2. Топология, где не присутствует внутренний коммутатор.

В зависимости от вашего сценария это соответствующие шаги:

**Если интерфейс ASA Management1/1 связан с внутренним коммутатором:**

Можно открыть сеанс в модуль и изменить его от ASA прежде, чем подключить его с внутренним коммутатором. Эта конфигурация позволяет вам обращаться к модулю SFR через IP путем размещения его в ту же подсеть как Внутренний интерфейс ASA с IP-адресом 10.0.0.254.

Линии полужирным являются определенными для данного примера и требуются для установления возможности подключения с помощью IP-адреса.

Линии курсивом будут варьироваться средой.

```
asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA5506W v5.4.1 (build 211)
Sourcefire3D login: admin
Password: Sourcefire

<<Output Truncated - you will see a large EULA>>

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.0.0.254Enter an IPv4
netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface []: 10.0.0.1
Enter a fully qualified hostname for this system [Sourcefire3D]: Cisco_SFR
Enter a comma-separated list of DNS servers or 'none' []: 10.0.0.250
Enter a comma-separated list of search domains or 'none' [example.net]: example.net
If your networking information has changed, you will need to reconnect.

For HTTP Proxy configuration, run 'configure network http-proxy'

Applying 'Default Allow All Traffic' access control policy.
```

**Примечание:** Это может занять пару минут для политики контроля доступа по умолчанию для применения на модуль SFR. Как только это завершено, можно выйти из CLI модуля SFR и назад в ASA путем нажима CTRL + SHIFT + 6 + X (CTRL ^ X)

**Если ASA НЕ связан с внутренним коммутатором:**

Внутренний коммутатор может не существовать в некоторых небольших развертываниях. В этом типе топологии клиенты обычно соединялись бы с ASA через интерфейс WiFi. В этом сценарии это возможно, избавляют от необходимости внешнего коммутатора и обращаются к модулю SFR через отдельный интерфейс ASA путем перекрестного подключения интерфейса Management1/1 к другому физическому интерфейсу ASA.

В данном примере физическое подключение по технологии Ethernet должно существовать между интерфейсом ASA GigabitEthernet1/3 и интерфейсом Management1/1. Затем, вы настраиваете ASA и модуль SFR, чтобы быть на отдельной подсети, и затем вы в состоянии обратиться к SFR от обоих ASA, а также клиенты, расположенные на интерфейсах Wi-Fi или внутренней части.

**Конфигурация интерфейса ASA:**

```
asa(config)# interface gigabitEthernet 1/3
asa(config-if)# ip address 10.2.0.1 255.255.255.0
asa(config-if)# nameif sfr
```

INFO: Security level for "sfr" set to 0 by default.

```
asa(config-if)# security-level 100
```

```
asa(config-if)# no shut
```

## Конфигурация модуля SFR:

```
asa# session sfr console
```

Opening console session with module sfr.

Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA5506W v5.4.1 (build 211)

Sourcefire3D login: admin

Password: Sourcefire

<<Output Truncated - you will see a large EULA>>

Please enter 'YES' or press <ENTER> to AGREE to the EULA: YES

System initialization in progress. Please stand by.

You must change the password for 'admin' to continue.

Enter new password:

Confirm new password:

You must configure the network to continue.

You must configure at least one of IPv4 or IPv6.

Do you want to configure IPv4? (y/n) [y]: y

Do you want to configure IPv6? (y/n) [n]: n

Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

**Enter an IPv4 address for the management interface [192.168.45.45]: 10.2.0.254**

**Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0**

**Enter the IPv4 default gateway for the management interface []: 10.2.0.1**

Enter a fully qualified hostname for this system [Sourcefire3D]: Cisco\_SFR Enter a comma-separated list of DNS servers or 'none' []: 10.0.0.250 Enter a comma-separated list of search domains or 'none' [example.net]: example.net If your networking information has changed, you will need to reconnect. For HTTP Proxy configuration, run 'configure network http-proxy' Applying 'Default Allow All Traffic' access control policy.

**Примечание:** Это может занять пару минут для политики контроля доступа по умолчанию для применения на модуль SFR. Как только это завершено, можно выйти из CLI модуля SFR и назад в ASA путем нажима CTRL + SHIFT + 6 +X (CTRL ^ X).

Как только конфигурация SFR применяется, необходимо быть в состоянии пропинговать управление IP-адресами SFR от ASA:

```
asa# ping 10.2.0.254
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.0.254, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```
asa#
```

Если вы не можете пропинговать интерфейс успешно, проверьте конфигурацию и состояние физических подключений по технологии Ethernet.

## Шаг 8. Соединитесь с GUI AP, чтобы включить радио и установить другую конфигурацию WAP

На этом этапе у вас должно быть подключение для управления WAP через GUI HTTP, как обсуждено в Кратком руководстве по началу работы. Необходимо будет или перейти к IP-адресу интерфейса BVI WAP's от web-браузера клиента, который связан с внутренней сетью на 5506 Вт, или можно применить пример конфигурации и подключение к SSID

WAP. Если вы не используете CLI ниже, необходимо включить кабель Ethernet от клиента к интерфейсу Gigabit1/2 на ASA.

Если вы предпочитаете использовать CLI для настройки WAP, можно открыть сеанс в него от ASA и использовать конфигурацию данного примера. Это создает открытый SSID с названием 5506 Вт и 5506W\_5 ГГц так, чтобы можно было использовать беспроводного клиента, чтобы соединиться с и далее управлять WAP.

**Примечание:** После применения этой конфигурации вы захотите обратиться к GUI и применить безопасность к SSIDs так, чтобы был зашифрован беспроводной трафик.

## Конфигурация интерфейса командой строки WAP для одиночной беспроводной сети VLAN с помощью модифицировала диапазоны IP

```
dot11 ssid 5506W
    authentication open
    guest-mode
dot11 ssid 5506W_5Ghz
    authentication open
    guest-mode
!
interface Dot11Radio0
!
    ssid 5506W
!
interface Dot11Radio1
!
    ssid 5506W_5Ghz
!
interface BVI1
    ip address 10.1.0.254 255.255.255.0
ip default-gateway 10.1.0.1
!
interface Dot11Radio0
    no shut
!
interface Dot11Radio1
    no shut
```

С этого момента можно выполнить обычные шаги для завершения конфигурации WAP, и необходимо быть в состоянии обратиться к ней от web-браузера клиента, связанного с вышеупомянутым созданным SSID. Именем пользователя по умолчанию точки доступа является Cisco с паролем Cisco с капиталом C.

## Cisco ASA 5506-X Краткое руководство по началу работы серии

[http://www.cisco.com/c/en/us/td/docs/security/asa/quick\\_start/5506X/5506x-quick-start.html#pgfId-138410](http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410)

Необходимо использовать IP-адрес 10.1.0.254 вместо 192.168.10.2, как сообщили в Кратком руководстве по началу работы.

## Конфигурации

Итоговая конфигурация должна совпасть с выходными данными (предполагающий использование примера диапазоны IP иначе займите место соответственно:



## Конфигурация ASA

Интерфейсы:

**Примечание:** Если у вас нет внутреннего коммутатора, линии курсивом только применяются:

```
asa# sh run interface gigabitEthernet 1/2
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 10.0.0.1 255.255.255.0
asa# sh run interface gigabitEthernet 1/3
!
interface GigabitEthernet1/3
 nameif sfr
 security-level 100
 ip address 10.2.0.1 255.255.255.0
asa# sh run interface gigabitEthernet 1/9
!
interface GigabitEthernet1/9
 nameif wifi
 security-level 100
 ip address 10.1.0.1 255.255.255.0
asa#
```

DHCP:

```
asa# sh run dhcpd
dhcpd auto_config outside **auto-config from interface 'outside' **auto_config dns x.x.x.x
x.x.x.x <-- these lines will depend on your ISP **auto_config domain isp.domain.com <-- these
lines will depend on your ISP ! dhcpd address 10.0.0.2-10.0.0.100 inside dhcpd dns 10.0.0.250
interface inside dhcpd enable inside ! dhcpd address 10.1.0.2-10.1.0.100 wifi dhcpd dns
10.0.0.250 interface wifi dhcpd enable wifi !
asa#
```

HTTP:

```
asa# show run http
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
asa#
```

## Aironet Конфигурация WAP (без config SSID в качестве примера)

```
asa# session wlan console
ap>enable
Password: Cisco
ap#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
ap#show configuration | include default-gateway
ip default-gateway 10.1.0.1
```

```
ap#show configuration | include ip route
ip route 0.0.0.0 0.0.0.0 10.1.0.1
ap#show configuration | i interface BVI|ip address 10
interface BVI1 ip address
10.1.0.254 255.255.255.0
```

## Конфигурация модуля FirePOWER (с внутренним коммутатором)

```

asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show network
===== [ System Information ] =====
Hostname           : Cisco_SFR
Domains            : example.net
DNS Servers        : 10.0.0.250
Management port    : 8305

IPv4 Default route
  Gateway           : 10.0.0.1

===== [ eth0 ] =====
State              : Enabled
Channels           : Management & Events
Mode               :
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : B0:AA:77:7C:84:10

----- [ IPv4 ] ----- Configuration : Manual
Address           : 10.0.0.254
Netmask          : 255.255.255.0
Broadcast        : 10.0.0.255
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

>

```

## Конфигурация модуля FirePOWER (без внутреннего коммутатора)

```

asa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
> show network
===== [ System Information ] =====
Hostname           : Cisco_SFR
Domains            : example.net
DNS Servers        : 10.0.0.250
Management port    : 8305

IPv4 Default route
  Gateway           : 10.2.0.1

===== [ eth0 ] =====
State              : Enabled
Channels           : Management & Events
Mode               :
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : B0:AA:77:7C:84:10

----- [ IPv4 ] -----
Configuration    : Manual
Address           : 10.2.0.254
Netmask          : 255.255.255.0
Broadcast        : 10.2.0.255
----- [ IPv6 ] -----
Configuration      : Disabled

```

```
=====[ Proxy Information ]=====  
State : Disabled  
Authentication : Disabled  
  
>
```

## Проверка

Чтобы проверить, что у вас есть правильное подключение к WAP для завершения процесса установки:

1. Подключите своего тестового клиента с Внутренним интерфейсом ASA и гарантируйте, что он получает IP-адрес от ASA через DHCP, который является в желаемом диапазоне IP.
2. Используйте web-браузер на своем клиенте, чтобы перейти к <https://10.1.0.254> и проверить, что GUI AP теперь доступен.
3. Пропингуйте интерфейс управления SFR от внутреннего клиента и ASA для проверки правильного подключения.

## Настройте DHCP со множественными беспроводными сетями VLAN

Конфигурация предполагает использование одиночной беспроводной сети VLAN. Виртуальный интерфейс моста (BVI) на беспроводном AP может предоставить мост для Несколько интерфейсов VLAN. Из-за синтаксиса для DHCP на ASA, если вы хотите настроить 5506 Вт как сервер DHCP для несколько интерфейсов VLAN, необходимо создать подинтерфейсы на Gigabit1/9, взаимодействуют и дают каждому название. Этот раздел ведет вас посредством процесса того, как удалить конфигурацию по умолчанию и применять конфигурацию, необходимую для настраивания ASA как сервера DHCP для несколько интерфейсов VLAN.

### Шаг 1. Удалите Существующую конфигурацию DHCP на Gig1/9

Во-первых, удалите существующую конфигурацию DHCP на Gig1/9 (Wi-Fi) интерфейс:

```
ciscoasa# no dhcpd address 10.1.0.2-10.1.0.100 wifi  
ciscoasa# no dhcpd enable wifi
```

### Шаг 2. Создайте подинтерфейсы для каждой VLAN на Gig1/9

Для каждой VLAN, которую вы настроили на точке доступа, необходимо настроить подинтерфейс Gig1/9. В конфигурации данного примера вы добавляете два подинтерфейса:

- Gig1/9.5, который будет иметь nameif vlan5 и будет соответствовать VLAN 5 и подсети 10.5.0.0/24.

- Gig1/9.30, который будет иметь nameif vlan30 и будет соответствовать VLAN 30 и подсети 10.3.0.0/24.

На практике важно, что VLAN и подсеть настроили, здесь совпадают с VLAN и подсетью, заданной на точке доступа. Nameif и номер подинтерфейса могут быть чем-либо, что вы выбираете. См. Краткое руководство по началу работы, ранее упомянутое для ссылок для

настройки точки доступа с помощью веб-GUI.

```
ciscoasa(config)# interface g1/9.5
ciscoasa(config-if)# vlan 5
ciscoasa(config-if)# nameif vlan5
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.5.0.1 255.255.255.0

ciscoasa(config-if)# interface g1/9.30
ciscoasa(config-if)# vlan 30
ciscoasa(config-if)# nameif vlan30
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.30.0.1 255.255.255.0
```

### Шаг 3. Определяйте пул DHCP для каждой VLAN

*Создайте отдельный пул DHCP для каждой настраиваемой VLAN. Синтаксис для этой команды требует, чтобы вы перечислили nameif, из которого ASA будет служить рассматриваемому пулу. Замеченный в данном примере, который использует VLAN 5 и 30:*

```
ciscoasa(config)# dhcpd address 10.5.0.2-10.5.0.254 vlan5
ciscoasa(config)# dhcpd address 10.30.0.2-10.30.0.254 vlan30
ciscoasa(config)# dhcpd enable vlan5
ciscoasa(config)# dhcpd enable vlan30
```

### Шаг 4. . Настройте точку доступа SSIDs, сохраните config и перезагрузите модуль

Наконец, точка доступа должна быть настроена для соответствия конфигурации ASA. Графический интерфейс пользователя (GUI) для точки доступа позволяет вам настраивать VLAN на AP через клиента, связанного с ASA в (Gigabit1/2) интерфейс. Однако, если вы предпочитаете использовать CLI, чтобы настроить AP через сеанс консоли ASA и затем соединиться с помощью беспроводных технологий для управления AP, можно использовать эту конфигурацию в качестве шаблона для создания двух SSIDs на VLAN 5 и 30. Это должно быть введено в консоли AP в режиме глобальной конфигурации:

```
dot11 vlan-name VLAN30 vlan 30
dot11 vlan-name VLAN5 vlan 5
!
dot11 ssid SSID_VLAN30
    vlan 30
    authentication open
    mbssid guest-mode
!
dot11 ssid SSID_VLAN5
    vlan 5
    authentication open
    mbssid guest-mode
!
interface Dot11Radio0
!
    ssid SSID_VLAN30
!
    ssid SSID_VLAN5
    mbssid
!
interface Dot11Radio0.5
    encapsulation dot1Q 5
    bridge-group 5
    bridge-group 5 subscriber-loop-control
    bridge-group 5 spanning-disabled
    bridge-group 5 block-unknown-source
    no bridge-group 5 source-learning
```

```

no bridge-group 5 unicast-flooding
!
interface Dot11Radio0.30
encapsulation dot1Q 30
bridge-group 30
bridge-group 30 subscriber-loop-control
bridge-group 30 spanning-disabled
bridge-group 30 block-unknown-source
no bridge-group 30 source-learning
no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
!
ssid SSID_VLAN30
!
ssid SSID_VLAN5
mbssid
!
interface Dot11Radio1.5
encapsulation dot1Q 5
bridge-group 5
bridge-group 5 subscriber-loop-control
bridge-group 5 spanning-disabled
bridge-group 5 block-unknown-source
no bridge-group 5 source-learning
no bridge-group 5 unicast-flooding
!
interface Dot11Radio1.30
encapsulation dot1Q 30
bridge-group 30
bridge-group 30 subscriber-loop-control
bridge-group 30 spanning-disabled
bridge-group 30 block-unknown-source
no bridge-group 30 source-learning
no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0.5
encapsulation dot1Q 5
bridge-group 5
bridge-group 5 spanning-disabled
no bridge-group 5 source-learning
!
interface GigabitEthernet0.30
encapsulation dot1Q 30
bridge-group 30
bridge-group 30 spanning-disabled
no bridge-group 30 source-learning
!
interface BVI1
ip address 10.1.0.254 255.255.255.0
ip default-gateway 10.1.0.1
!
interface Dot11Radio0
no shut
!
interface Dot11Radio1
no shut

```

*На этом этапе конфигурация управления ASA и AP должна быть завершена, и действия ASA как сервер DHCP для VLAN 5 и 30. После сохранения конфигурации с помощью команды **write memory** на AP, если у вас все еще есть проблемы с подключением тогда, необходимо повторно загрузить AP с помощью команды **повторной загрузки** от CLI. Однако при получении IP-адреса на недавно созданном SSIDs тогда, никакие дальнейшие действия не требуются. `ap#write memory`*

```
Building configuration...  
[OK]  
ap#reload  
Proceed with reload? [confirm]  
Writing out the event log to flash:/event.log ...
```

**Примечание:** Вы не должны повторно загружать все устройство ASA.  
Необходимо только повторно загрузить встроенную точку доступа.

Как только AP заканчивает перезагружаться, тогда у вас должно быть подключение к GUI AP от клиентского компьютера на Wi-Fi или внутренних сетях. Обычно требуется приблизительно две минуты для AP к полностью перезагрузке. С этого момента можно применить обычные шаги для завершения конфигурации WAP.

**Cisco ASA 5506-X Краткое руководство по началу работы серии**

[http://www.cisco.com/c/en/us/td/docs/security/asa/quick\\_start/5506X/5506x-quick-start.html#pgfid-138410](http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfid-138410)

## Устранение неполадок

Устранение проблем подключения ASA выходит за рамки этого документа, так как это предназначено для начальной конфигурации. См. сверение и разделы конфигурации, чтобы гарантировать, что были должным образом выполнены все шаги.