Настройка облегченной точку доступа как запрашивающего устройства 802.1x

Содержание

Введение

Этот документ описывает, как настроить Облегченную точку доступа как соискатель 802.1x для аутентификации против сервера RADIUS.

Предварительные условия

Требования

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

- Cisco Aironet 1130, 1240, или точка доступа серии 1250
- WLC, который выполняет IOS® Version 5.1
- Коммутаторы Cisco Catalyst серии 3560 с Cisco IOS Release 12.2 (35) SE5
- Коммутаторы Cisco Catalyst серии 3750 с Cisco IOS Release 12.2 (40) SE
- Коммутаторы Cisco Catalyst серии 4500 с Cisco IOS Release 12.2 (40) SG
- Коммутаторы Cisco Catalyst серии 6500 с Supervisor Engine 32, который выполняет Cisco IOS Release 12.2 (33) SXH

Используемые компоненты

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.

Общие сведения

LAP имеют установленные сертификаты X.509 фабрики, подписанные секретным ключом, которые врезаются в устройство во время изготовления. LAP используют этот сертификат для аутентификации с WLC при процессе соединения. Для получения дополнительной информации обратитесь к Обеспечению Плоскости Управления LWAPP Развертывания документа Контроллеры беспроводной локальной сети Cisco 440X Series. Этот метод описывает другой способ аутентифицировать LAP. С Версией 5.1 WLC можно настроить аутентификацию 802.1x между точкой доступа Cisco Aironet и коммутатором Cisco. Точка доступа действует как соискатель 802.1x и аутентифицируется коммутатором против сервера RADIUS (ACS), который использует EAP-FAST с анонимной инициализацией PAC. Как только это настроено для аутентификации 802.1x, коммутатор не позволяет трафику кроме трафика 802.1x проходить через порт, пока устройство, связанное с портом, не аутентифицируется успешно. Точка доступа может аутентифицироваться или прежде чем она присоединится к WLC или после того, как она присоединилась к WLC, в этом случае вы настраиваете 802.1x на коммутаторе после того, как LAP присоединяется к WLC.

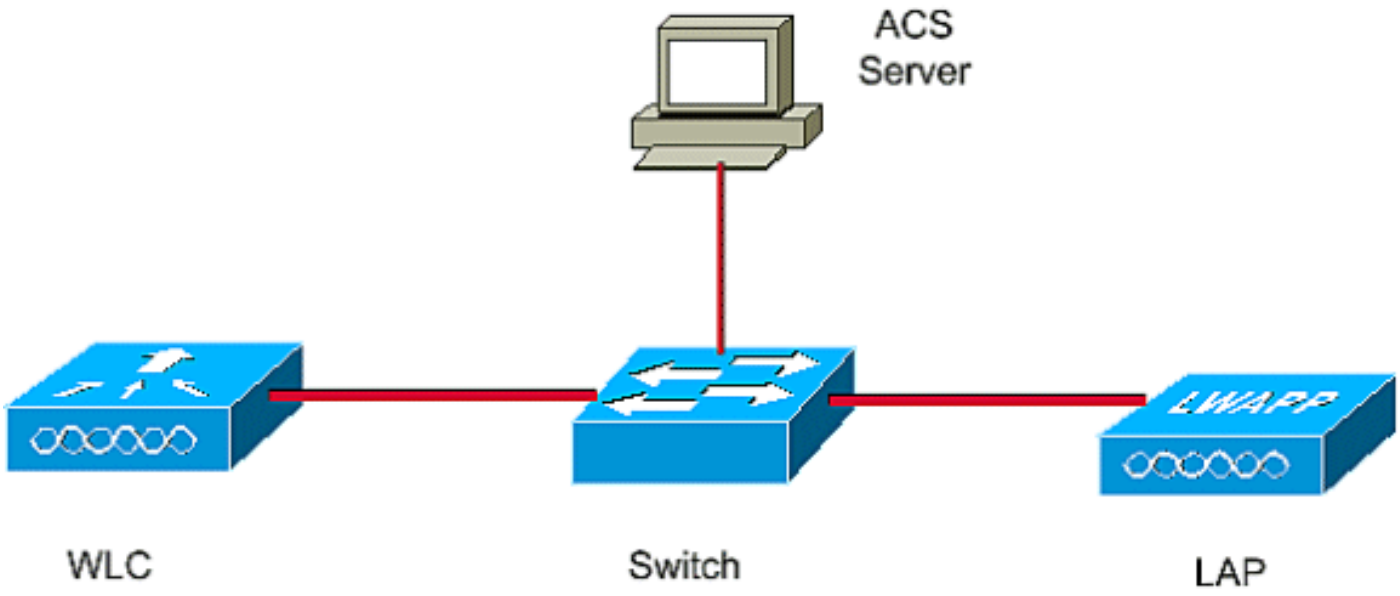
Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Этот документ использует эти IP-адреса:

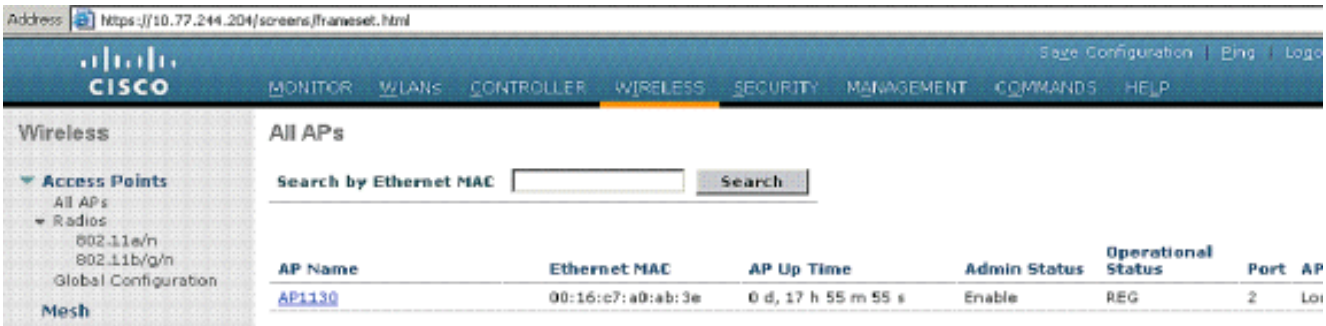
- IP-адрес коммутатора 10.77.244.210
- IP-адрес сервера ACS 10.77.244.196
- IP-адрес WLC 10.77.244.204

Настройте LAP

В этом разделе вам предоставляют информацию по настройке LAP как соискатель 802.1x.

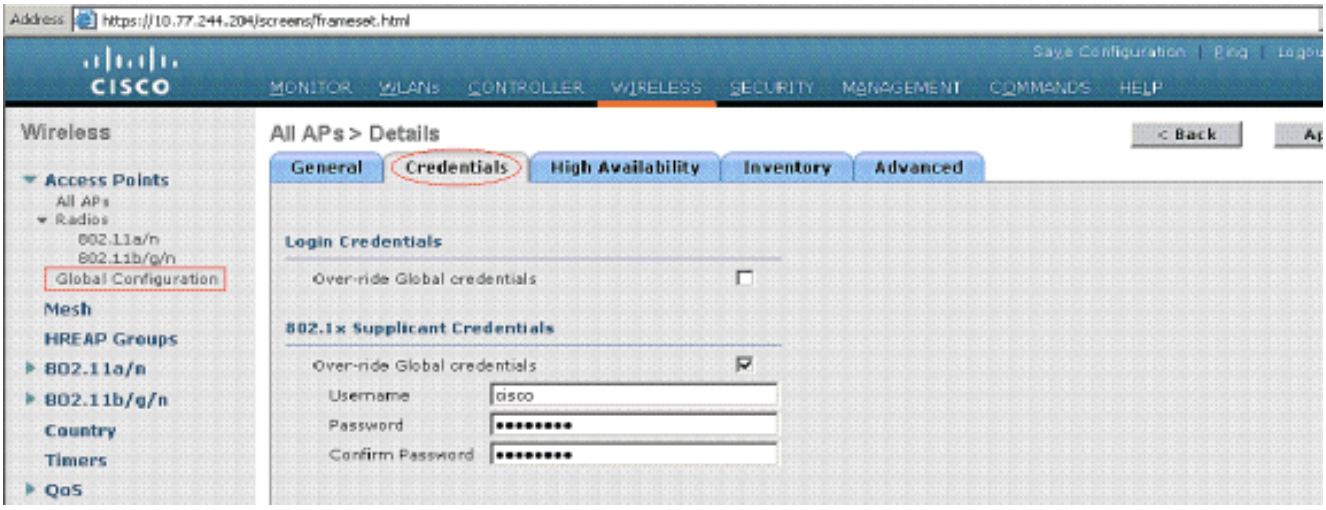
Выполните следующие действия:

1. Удостоверьтесь, что точка доступа загружена Легковесным Образом для восстановления.
2. Подключите LAP с коммутатором.
3. LAP проходит процесс соединения и регистрируется в WLC. Это может быть проверено из меню Wireless WLC как показано на рисунке 1.**Рисунок 1**



4. Нажмите **точку доступа** и нажмите вкладку **Credentials**.
5. Под заголовком Учетных данных Соискателя 802.1x установите **Глобальный учетный** флажок **Замены** для установки имени пользователя и пароля 802.1x для этой точки доступа. Можно также установить имя пользователя и пароль вместе во все точки доступа, которые присоединяются к WLC с меню Global Configuration. Рисунок 2

показывает, как установить учетные данные 802.1x для точки доступа.**Рис. 2**



Примечание: Можно также установить имя пользователя и пароль 802.1x для точки доступа с **config ap dot1xuser добавляет <password> пароля <user> имени пользователя cisco_ap (название AP)** команды CLI WLC.

6. Нажмите **Apply** для фиксации изменений.
7. Нажмите **конфигурацию Save** для сохранения учетных данных.**Примечание:** После того, как сохраненный, эти учетные данные сохранены через WLC и перезагрузки точки доступа. Они изменяются только, когда LAP присоединяется к новому WLC. LAP принимает имя пользователя и пароль, которые были настроены на новом WLC.
8. Если точка доступа еще не присоединилась к WLC, необходимо подключиться с консоли в LAP, чтобы установить учетные данные и использовать эту команду CLI в режиме включения:`LAP#lwapp ap dot1x username <username> password <password>`
Примечание: Эта команда доступна только для точек доступа, которые выполняют 5.1 образов для восстановления.

Настройте коммутатор

Коммутатор действует как средство проверки подлинности для LAP и аутентифицирует LAP против сервера RADIUS. Если коммутатор не имеет совместимого программного обеспечения, обновите коммутатор. На CLI коммутатора введите эти команды для включения аутентификации 802.1x на порте коммутатора:

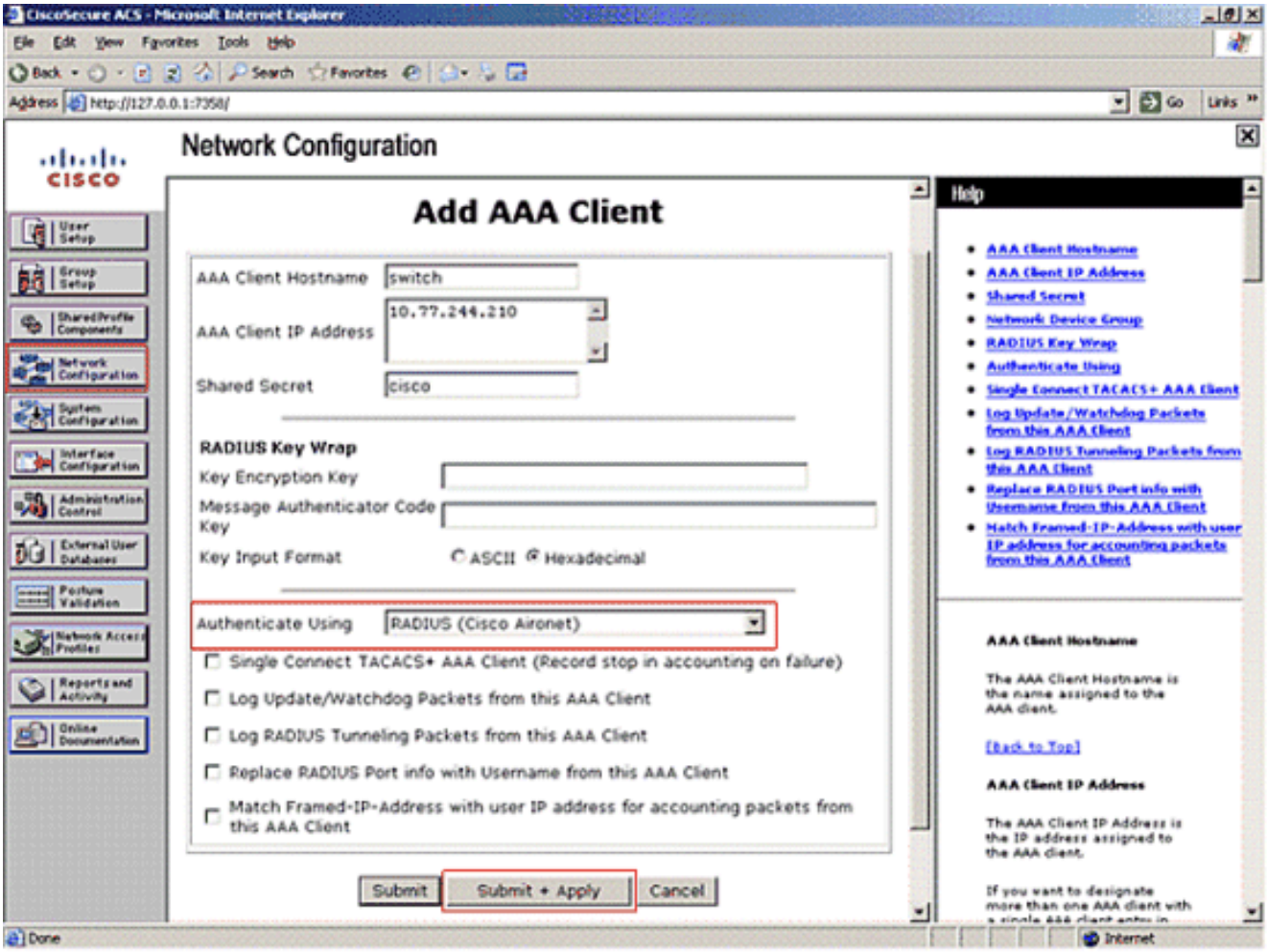
```
switch#configure terminal                    switch(config)dot1x system-auth-control
switch(config)aaa new-model                    switch(config)aaa authentication dot1x default
group radius                    switch(config)radius server host 10.77.244.196 key cisco!---
configures the radius server with shared secret switch(config)interface gigabitEthernet 1/0/43!-
-- 43 is the port number on which the access point is connected. switch(config-if)switchport
mode access switch(config-if)dot1x pae authenticator!--- configures dot1x authentication
switch(config-if)dot1x port-control auto!--- With this command switch initiates the 802.1x
authentication.
```

Настройка RADIUS-сервера

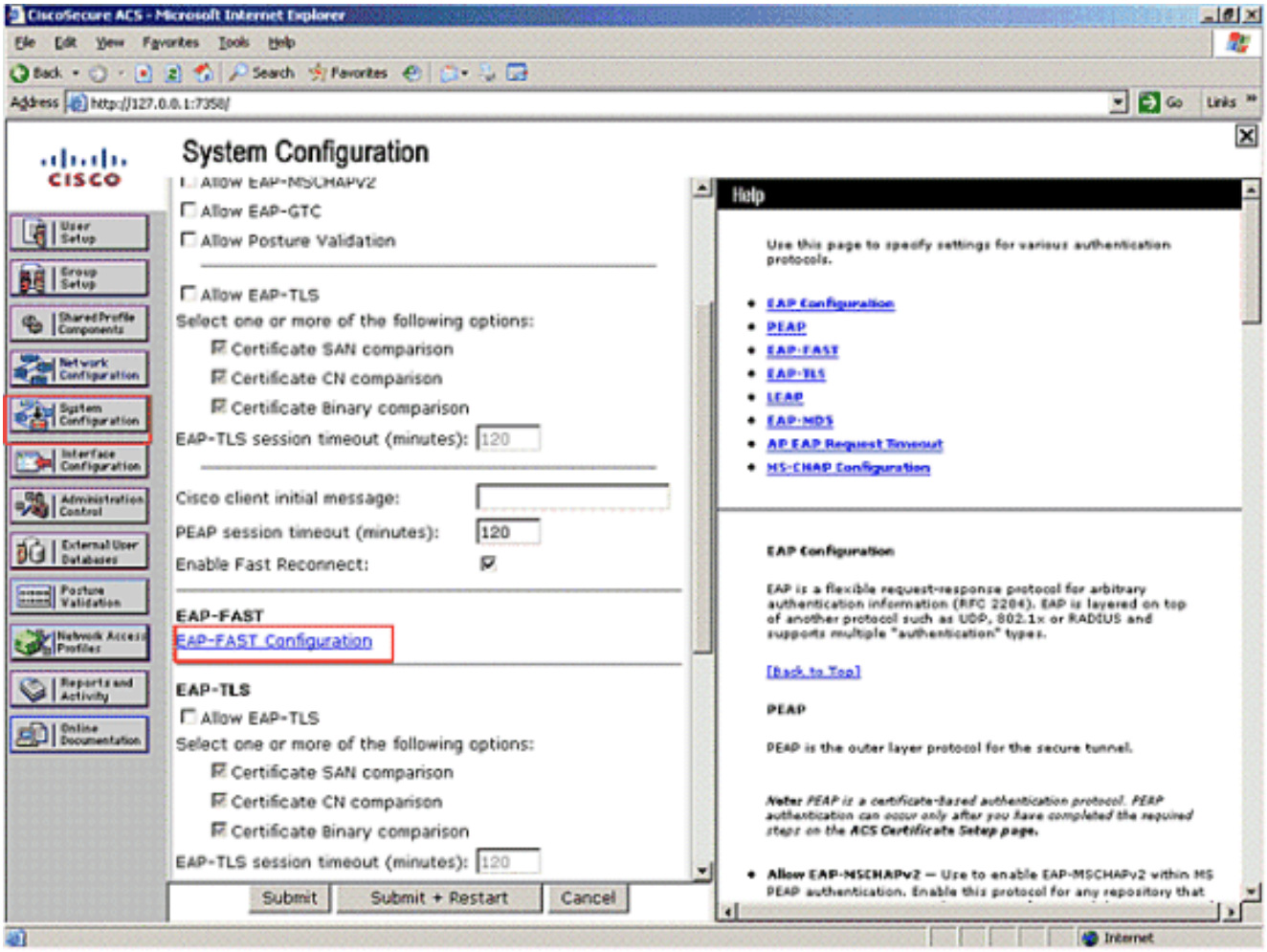
LAP аутентифицируется с EAP-FAST. Удостоверьтесь, что сервер RADIUS, который вы используете, поддерживает этот метод EAP. В данном примере сервер ACS используется для аутентификации. Выполните эти шаги на сервере ACS:

1. Запустите экран admin ACS.

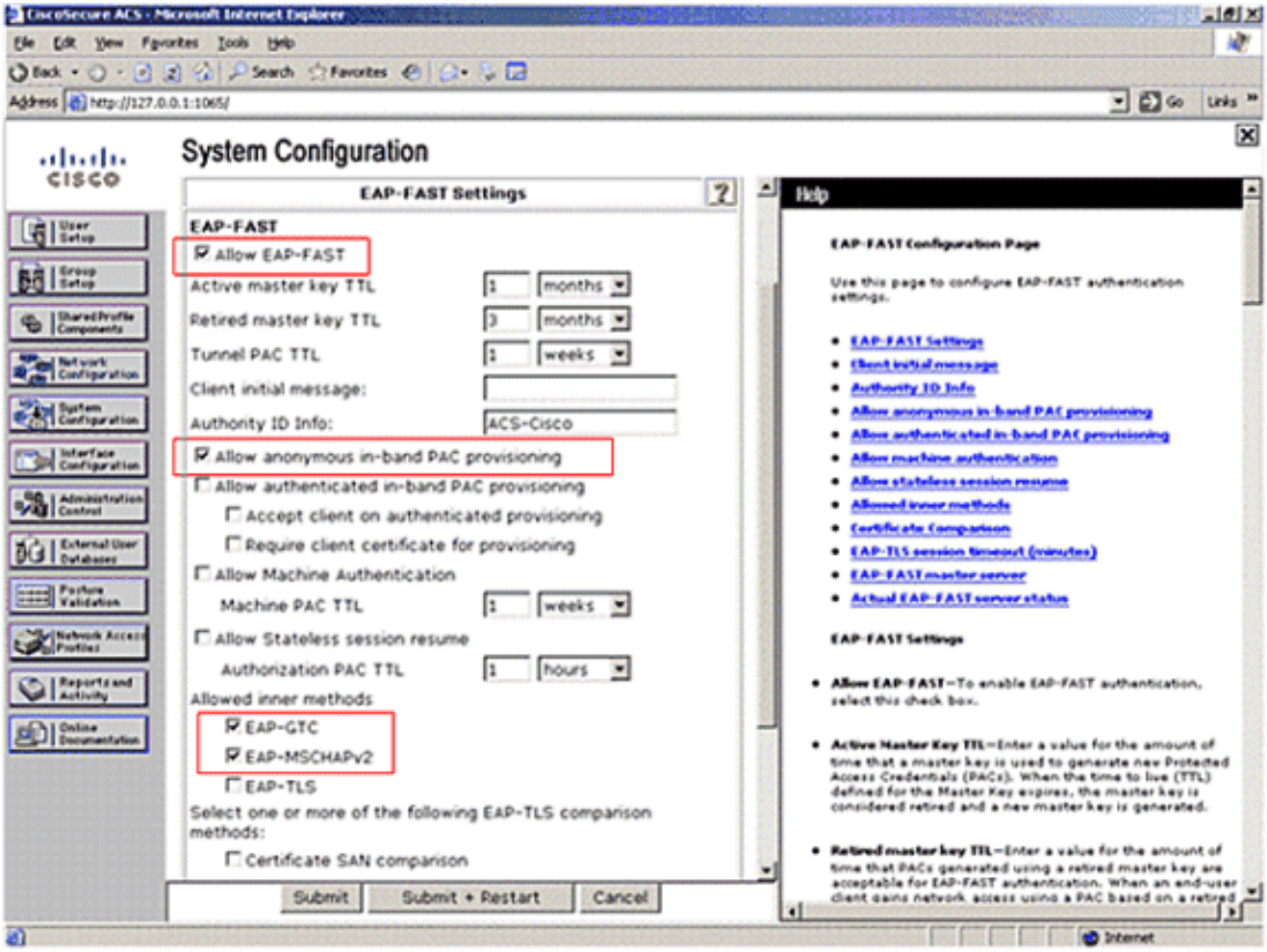
2. Настройте имя пользователя и пароль LAP в базе данных ACS. Для добавления учетной записи пользователя в ACS обратитесь к разделу Управления пользователями документа Руководство пользователя для сервера Cisco Secure Access Control Server 4.2.
3. Настройте Коммутатор как клиента AAA к серверу ACS. На экране admin ACS нажмите меню **Network Configuration**.
4. Под разделом **клиента AAA нажмите Add New Запись**. Введите эти параметры:Введите IP-адрес коммутатора в поле *AAA Client IP Address*.Введите общий секретный ключ коммутатора. Это должно быть точно тем же на коммутаторе и сервере ACS.Выберите **RADIUS Protocol** в поле *Authenticate Using*. По умолчанию это - TACACS +.**Примечание:** Проверьте сервер ACS для описания Протоколов RADIUS.См. рис. 3.**Рис. 3**



5. Нажмите **Submit + Применяются** для сохранения клиента AAA.
6. EAP-FAST должен быть включен на сервере RADIUS. Нажмите меню **System Configuration** в левой стороне. Нажмите **Опцию настройки Глобальной аутентификации**.**Рис. 4**



7. Нажмите **EAP - Конфигурация FAST** как показано на рисунке 4.
8. На Странице настроек EAP-FAST установите **Позволять** флажок **EAP-FAST**. LAP использует EAP-FAST с анонимной инициализацией PAC. Проверьте **Позволение Анонимной внутриполосной** коробки **инициализации PAC**. Для получения дополнительной информации обратитесь к Аутентификации EAP-FAST документа с Примером конфигурации Внешнего сервера RADIUS и Контроллерами беспроводной локальной сети.**Рис. 5**



9. Удостоверьтесь, что **EAP-GTC** и **EAP-MSCHAPv2** проверены под, *Позволяют внутренние методы*. Рисунок 5 показывает пример конфигурации шагов 8 и 9.

Проверка

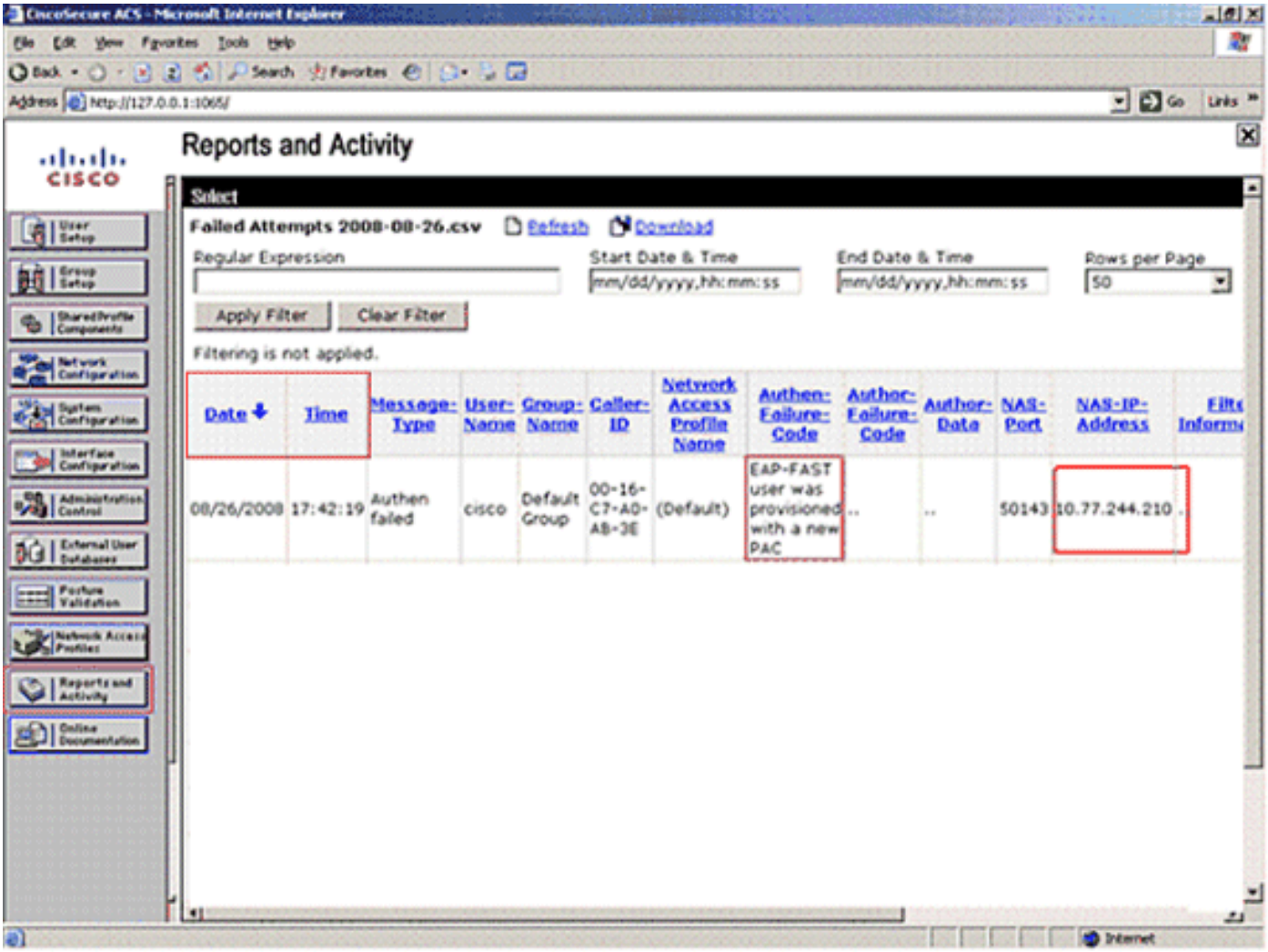
Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

Как только 802.1x включен на порте коммутатора, весь трафик кроме трафика 802.1x заблокирован через порт. LAP, который уже зарегистрирован к WLC, разъединен. Только после того, как успешная аутентификация 802.1x является другим трафиком, позволенным проходить. Успешная регистрация LAP к WLC после 802.1x включена на коммутаторе, указывает, что аутентификация LAP успешна.

Можно также проверить это от ACS. От основного экрана ACS нажмите меню **Reports и Authentication**. Нажмите опцию **Failed Attempts**. Если аутентификация успешна, вы находите, *что Опознавательное сообщение об ошибках* с *пользователем EAP-FAST* кода *было настроено с новым PAC с IP-адресом коммутатора* в поле NAS-IP-Address как показано на рисунке 6. Можно также подтвердить с Датой и времей аутентификации.

Рис. 6



Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

1. Используйте **команду ping** и проверку, если сервер ACS достижим от коммутатора.
2. Удостоверьтесь, что коммутатор настроен как клиент AAA на сервере ACS.
3. Гарантируйте, что общий секретный ключ является тем же между коммутатором и сервером ACS.
4. Проверьте, включен ли EAP-FAST на сервере ACS.
5. Проверьте для соответствия программного обеспечения на устройствах.
6. Проверьте, настроены ли учетные данные 802.1x для LAP и являются тем же на сервере ACS.**Примечание:** Имя пользователя и пароль учитывает регистр.

Команды для устранения неполадок

В настоящее время существуют команды no debug, доступные для этой функции.

Дополнительные сведения

- Управление облегченными точками доступа
- Настройка аутентификации на основе портов по стандарту IEEE 802.1x

- Cisco Systems – техническая поддержка и документация