

802.1x проводная аутентификация на коммутаторе серии Catalyst 3550 и примере конфигурации версии ACS 4.2

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Конфигурация коммутатора в качестве примера](#)

[Конфигурация AcS](#)

[Проверка](#)

[Устранение неполадок](#)

Введение

Этот документ предоставляет основному примеру конфигурации IEEE 802.1x Версию 4.2 Access Control Server (ACS) Cisco и протокол Набора удаленного доступа в сервисе пользователя (RADIUS) для проводной аутентификации.

Предварительные условия

Требования

Компания Cisco рекомендует следующее:

- Подтвердите возможности IP - доступы между ACS и коммутатором.
- Гарантируйте, что порты протокола пользовательских датаграмм (UDP) 1645 и 1646 открыты между ACS и коммутатором.

Используемые компоненты

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

- Cisco Catalyst 3550 Series Switches

- Версия 4.2 Cisco Secure ACS

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.

Настройка

Конфигурация коммутатора в качестве примера

1. Для определения сервера RADIUS и предварительного общего ключа, введите эту команду:

```
Switch(config)# radius-server host 192.168.1.3 key cisco123
```

2. Для добавления функциональности 802.1x введите эту команду:

```
Switch(config)# dot1x system-auth-control
```

3. Чтобы глобально - включить Аутентификацию, авторизацию и учет (AAA) и Проверку подлинности RADIUS и авторизацию, введите эти команды:

Примечание: Если необходимо передать атрибуты от сервера RADIUS, это необходимо; иначе, можно пропустить его.

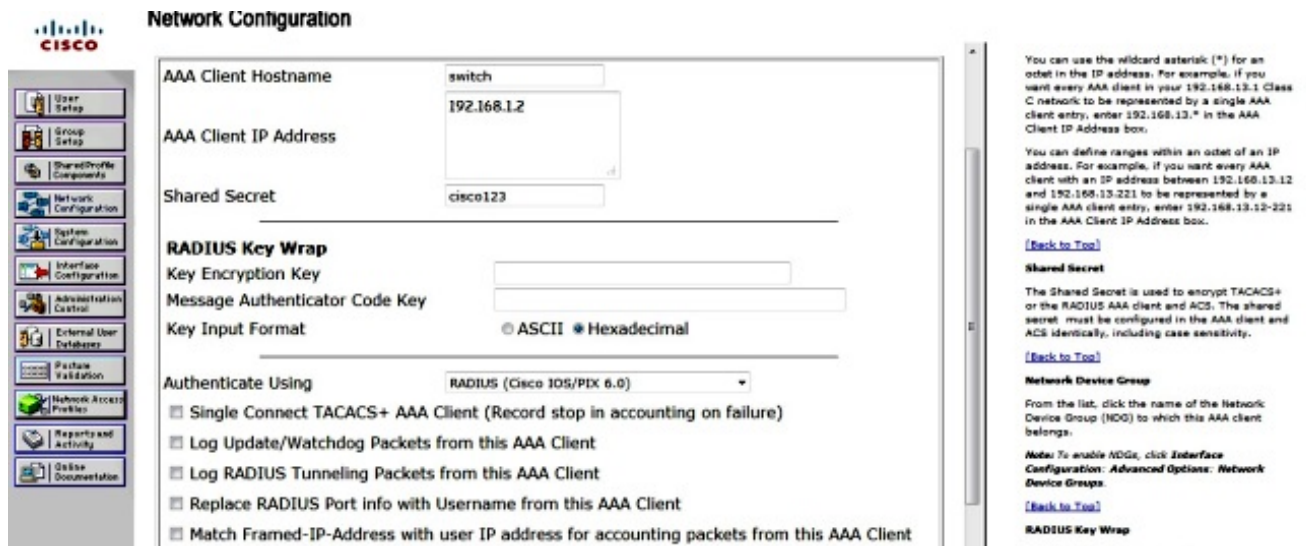
```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
switch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <vlan>
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period <seconds to wait after failed attempt>
Switch(config-if)# dot1x timeout tx-period <time to resubmit request>
```

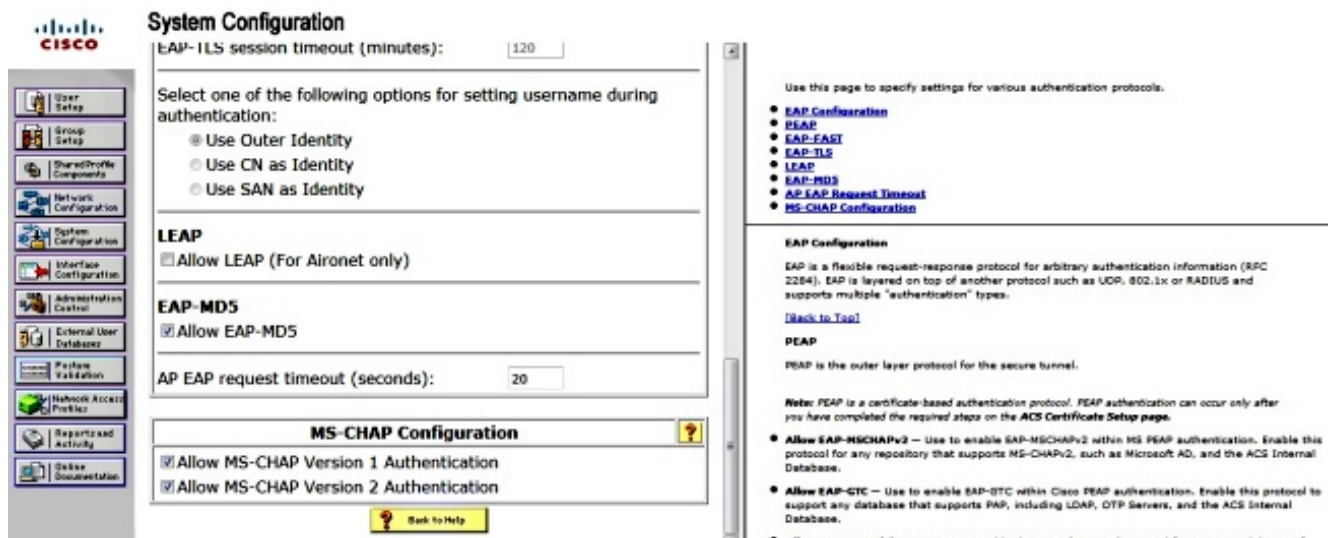
Конфигурация AcS

1. Для добавления коммутатора как клиент AAA в ACS перейдите к **Network Configuration>**, Добавляет клиент AAA записи и вводит эту информацию:

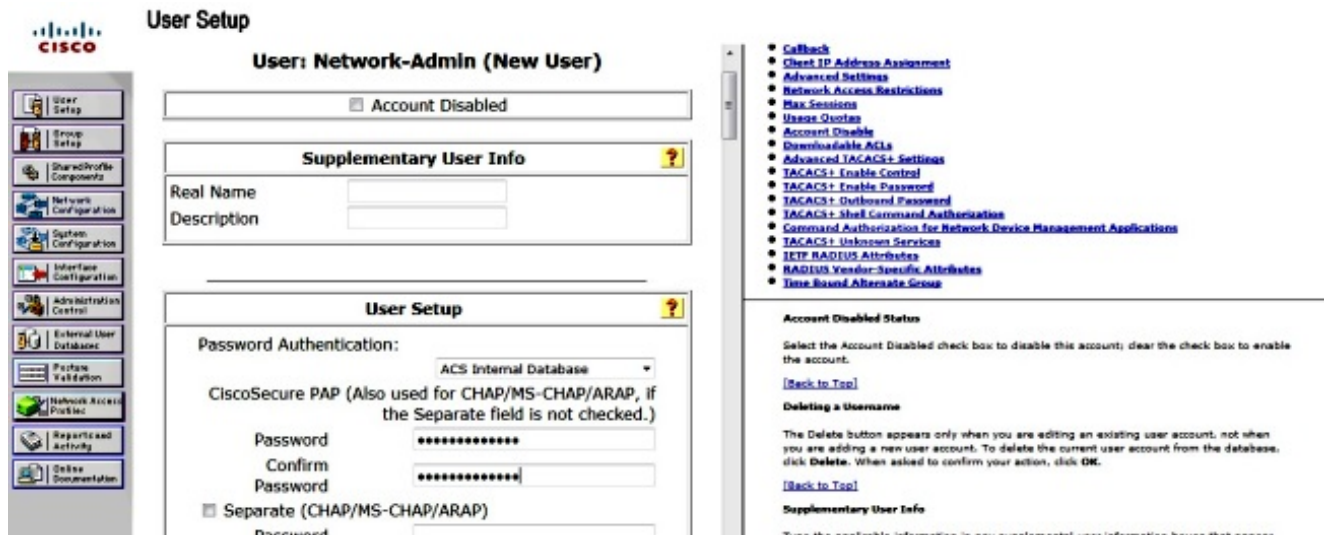
IP-адрес: <IP>Общий secret: <ключ>Используемая аутентификация: радиус (Cisco IOS®/PIX 6.0)



2. Для настройки опознавательной настройки перейдите к **Конфигурации системы** > **Настройка Глобальной аутентификации** и проверьте, что проверен флажок **Allow MS-CHAP Version 2 Authentication**:



3. Для настройки пользователя нажмите **User Setup** на меню и выполните эти шаги: Введите **Сведения о пользователе**: <username> Сетевого Admin. Нажмите **Add/Edit**. Введите **Настоящее имя**: Сетевой Admin <описательное имя>. Добавьте **Описание**: *выбор <your>*. Выберите проверку подлинности с помощью пароля: внутренняя база данных ACS. Ввести пароль:..... <password>. Подтвердите пароль: <password>. Нажмите кнопку **Submit** (Отправить).



Проверка

[Средство интерпретации выходных данных \(только зарегистрированные клиенты\)](#) поддерживает некоторые команды show. Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

Введите эти команды, чтобы подтвердить, что ваша конфигурация работает должным образом:

- show dot1x
- сводка show dot1x
- интерфейс show dot1x
- *<interface>* интерфейса show authentication sessions
- *<interface>* show authentication interface

```
Switch(config)# show dot1x
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

```
Switch(config)# show dot1x summary
```

```
Interface PAE Client Status
```

```
Fa0/4 AUTH
```

```
Switch(config)# show dot1x interface fa0/4 detail
```

```
Dot1x Info for FastEthernet0/4
```

```
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

Устранение неполадок

Этот раздел предоставляет команды отладки, которые можно использовать для устранения проблем конфигурации.

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

- `debug dot1x все`
- `debug authentication все`
- `debug radius` (предоставляет информацию радиуса в уровне отладки),
- `debug aaa authentication` (отлаживают для аутентификации),
- `debug aaa authorization` (отлаживают для авторизации),