Содержание

Введение

Доступ типа "замок и ключ" позволяет настраивать динамические списки доступа, предоставляющие каждому пользователю доступ к определенному хосту источника/назначения с помощью проверки подлинности пользователя. Пользовательский доступ предоставлен через Cisco IOS® Firewall динамично без любого компромисса в ограничениях безопасности.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. В этом случае лабораторная среда состояла из 2620 маршрутизаторов рабочий релиз 12.3 программного обеспечения Cisco IOS (1). Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Обсуждение спуфинга

Доступ по динамическим спискам позволяет внешнему событию размещать открытие в межсетевой экран Cisco IOS. Если это открытие существует, маршрутизатор становится чувствителен к спуфингу адреса источника. Для предотвращения этого предоставьте поддержке шифрования с помощью шифрования IP с аутентификацией или шифрования.

Спуфинг – это проблема со всеми существующими списками доступа. Доступ "замок и ключ" не решает эту проблему.

Поскольку при доступе с системой "замки и ключи" появляется потенциальный путь через межсетевой экран, необходимо подумать о динамическом доступе. Другой хост, имитируя ваш адрес с проверенной подлинностью, получает доступ позади межсетевого экрана. При динамическом доступе есть возможность, что неавторизованный узел сети, подделавший ваш аутентифицированный адрес, получает доступ за межсетевой экран. Доступ по динамическим спискам не вызывает проблему подмены адреса. Проблема определяется здесь только как проблема для пользователя.

Производительность

На производительность влияют в этих двух ситуациях.

- Каждый динамический список доступа принудительно делает перестроение списка доступа на кремниевом устройстве коммутации (SSE). Это мгновенно приводит к замедлению коммутируемого пути SSE.
- Динамические списки доступа требуют средства времени простоя (даже если таймаут оставляют принять значение по умолчанию). Поэтому динамическими списками доступа не может быть коммутированный SSE. Эти записи обрабатываются в пути быстрой коммутации протокола.

Наблюдайте конфигурации граничного маршрутизатора. Удаленные пользователи создают записи списка доступа на граничном маршрутизаторе. Список доступа растет и уменьшается динамично. Записи динамически удаляются из списка после истечения либо периода бездействия, либо максимального времени ожидания. Крупные списки доступа ведут к снижению эффективности коммутации пакетов.

Когда использовать доступ с системой замков и ключей

Здесь перечислены два примера, когда вы используете доступ типа замок-и-ключ:

- Когда вы хотите, чтобы удаленный хост был в состоянии обратиться к хосту в вашем объединении нескольких локальных сетей через Интернет. Доступ по динамическим спискам ограничивает доступ вне вашего межсетевого экрана на отдельном хосте или сетевом основании.
- При необходимости подключения поднабора хостов сети к хосту удаленной сети, защищенной межсетевым экраном. Имея доступ “замок и ключ”, можно включить только

необходимый набор хостов для получения доступа путем их аутентификации через сервер TACACS+ или RADIUS.

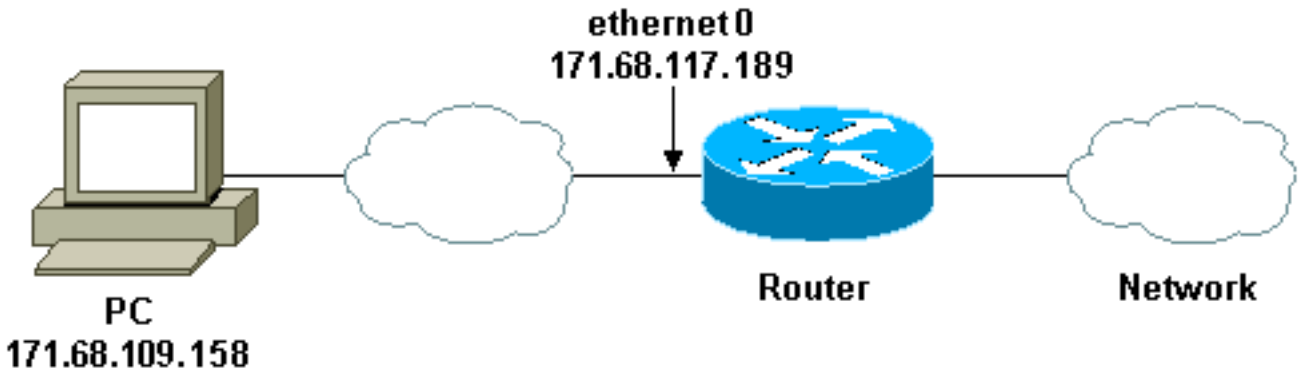
Операция доступа с помощью технологии Lock-and-Key

Этот процесс описывает операцию доступа замок и ключ.

1. Пользователь открывает сеанс Telnet для пограничного маршрутизатора, настроенного для доступа типа "замок и ключ".
2. Программное обеспечение Cisco IOS получает пакет Telnet. Это выполняет процесс проверки подлинности пользователя. Пользователь должен пройти аутентификацию, прежде чем вход будет разрешен. Процесс проверки подлинности сделан маршрутизатором или центральным сервером доступа, таким как TACACS + или сервер RADIUS.

Типовая конфигурация и устранение неполадок

Схема сети



Cisco рекомендует вам использовать сервер TACACS+ для обработки ваших запросов об аутентификации. TACACS+ предоставляет службы аутентификации, авторизации и учета. Это также предоставляет поддержку протокола, спецификацию протокола и централизованную базу данных безопасности.

Можно аутентифицировать пользователя на маршрутизаторе или с TACACS + или сервер RADIUS.

Примечание: Эти команды глобальные, если не указано обратное.

На маршрутизаторе вам нужно **имя пользователя** для пользователя для локальной проверки подлинности.

```
username test password test
```

Наличие команды login local в строках vty делает необходимым использование username.

```
line vty 0 4login local
```

Если вы не доверяете пользователя для запуска **команды access-enable**, можно сделать одну из двух вещей:

- Сопоставьте время ожидания с пользователем для каждого пользователя.**username test autocommand access-enable host timeout 10** ИЛИ
- Вынудите всех пользователей что Telnet в иметь тот же таймаут.**line vty 0 4login localautocommand access-enable host timeout 10**

Примечание: 10 в синтаксисе являются *временем простоя* списка доступа. Это отвергнуто абсолютным временем ожидания в динамическом списке доступа.

Определите расширенный список доступа, который применен, когда пользователь (любой пользователь) входит в маршрутизатор, и **команда access-enable** выполнена. Максимальное абсолютное время для этой "дыры" в фильтре установлено в 15 минут. После 15 минут дыра закрывает, использует ли кто-либо его. Название **testlist** должно существовать, но не является значительным. Ограничьте сети, к которым у пользователя есть доступ путем настройки адреса источника или назначения (здесь, пользователь не ограничен).

access-list 120 dynamic testlist timeout 15 permit ip any any

Определите список доступа, должен был заблокировать все кроме способности к Telnet в маршрутизатор (для открытия дыры, пользователю нужно к Telnet к маршрутизатору). IP-адресом здесь является IP-адрес Ethernet маршрутизатора.

access-list 120 permit tcp any host 171.68.117.189 eq telnet

Существует неявное**, запрещают все** в конце (не введенный здесь).

Примените этот список доступа к интерфейсу, на котором входят пользователи.

interface ethernet1 ip access-group 120 in

Вы сделаны.

Это - то, на что фильтр похож на маршрутизаторе прямо сейчас:

```
Router#show access-listsExtended IP access list 120 10 Dynamic testlist permit ip any any log 20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Пользователи, которые получают доступ к вашей внутренней сети, не в состоянии видеть что-либо пока они Telnet к маршрутизатору.

Примечание: 10 здесь являются *временем простоя* списка доступа. Это отвергнуто абсолютным временем ожидания в динамическом списке доступа.

```
%telnet 2514ATrying 171.68.117.189 ...Connected to 2514A.network.com.Escape character is '^]'.
User Access Verification Username: testPassword: testConnection closed by foreign host.
```

Фильтр похож на это.

```
Router#show access-listsExtended IP access list 120 10 Dynamic testlist permit ip any any log permit ip host 171.68.109.158 any log (time left 394) 20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Существует дыра в фильтре для этого пользователя на основе IP - адреса источника. Когда кто-то еще делает это, вы видите *две дыры*.

```
Router#show ip access-lists 120Extended IP access list 120 10 Dynamic testlist permit ip any any log permit ip host 171.68.109.64 any log permit ip host 171.68.109.158 any log 20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Эти пользователи в состоянии иметь завершенный IP - доступ к любому IP - адресу назначения от их *IP - адреса источника*.

Использование TACACS+

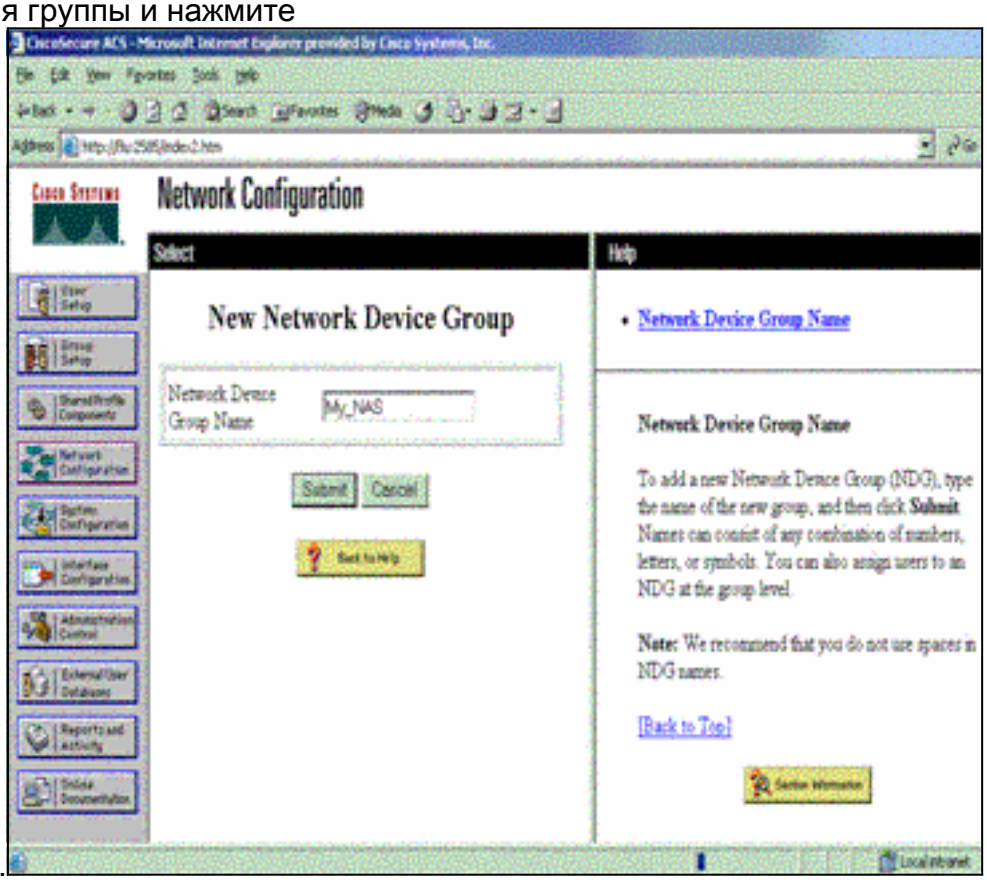
Настройте TACACS +

Настройте TACACS + сервер, чтобы вынудить проверку подлинности и авторизация быть сделанной на TACACS + сервер для использования TACACS +, как показано в выходных данных ниже:

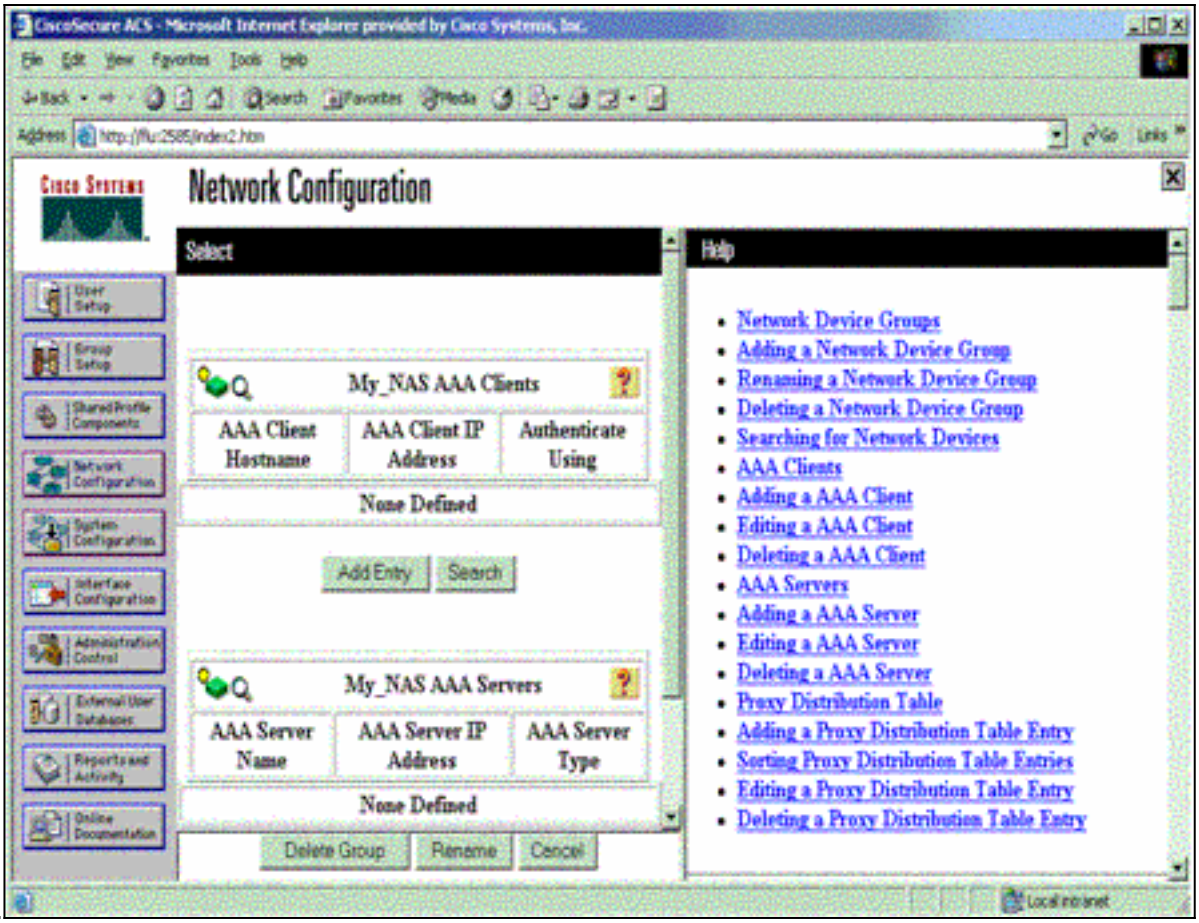
```
aaa new-model!!aaa authentication login default group tacacs+ localaaa authorization exec
default group tacacs+tacacs-server host 10.48.66.53 key cisco123
```

Выполните эти шаги для настройки TACACS + на Cisco Secure ACS для Windows:

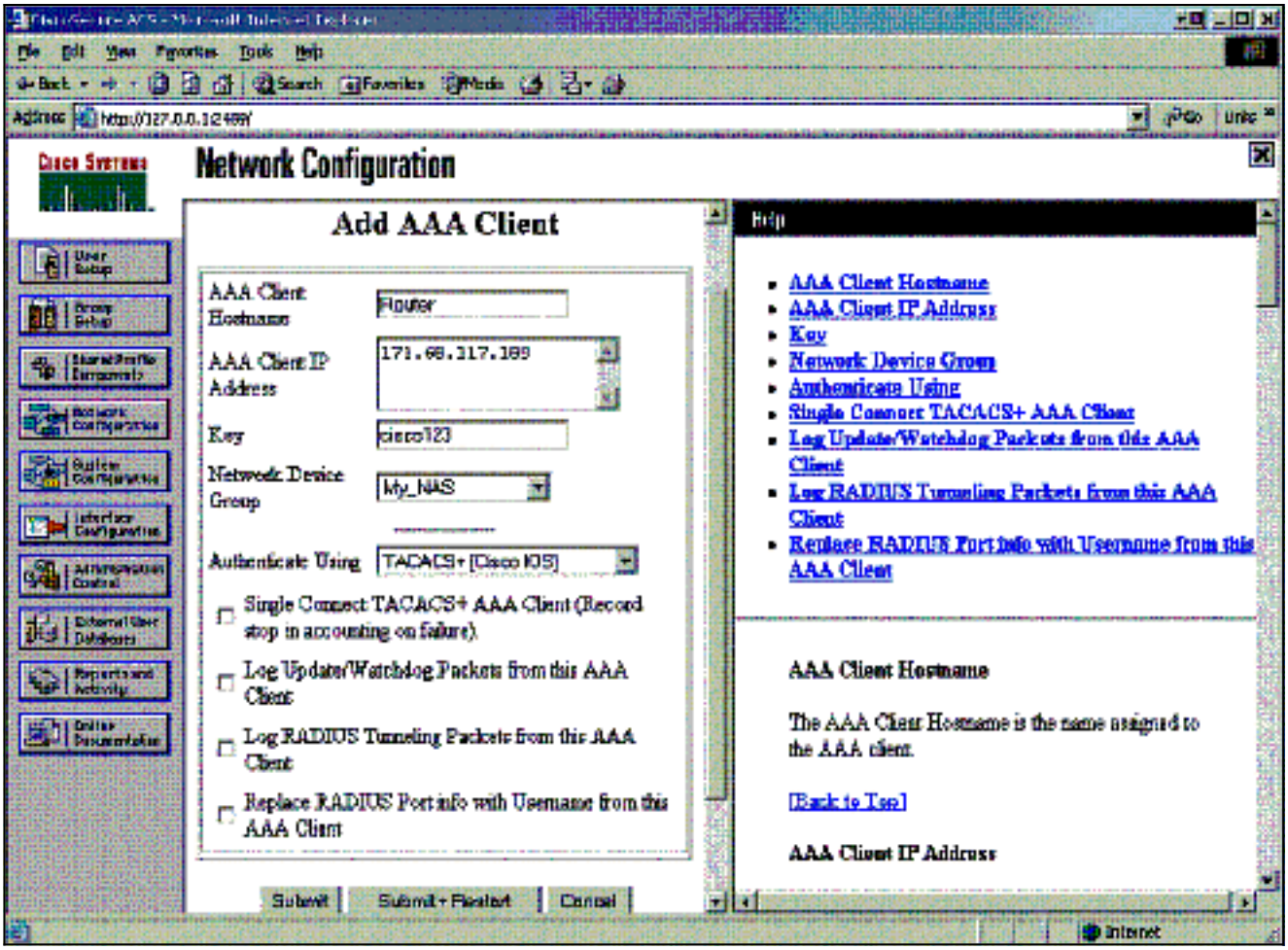
1. Откройте веб-браузер. Введите адрес своего сервера ACS, который находится в форме **http://*<IP_address или DNS_name>*:2002**. (Данный пример использует порт по умолчанию 2002.) Входят как admin.
2. **Выберите Network Configuration (Настройка сети). Нажмите Add Запись** для создания Группы сетевых устройств, которая содержит серверы доступа к сети (NAS). Введите имя для группы и нажмите **Submit**.



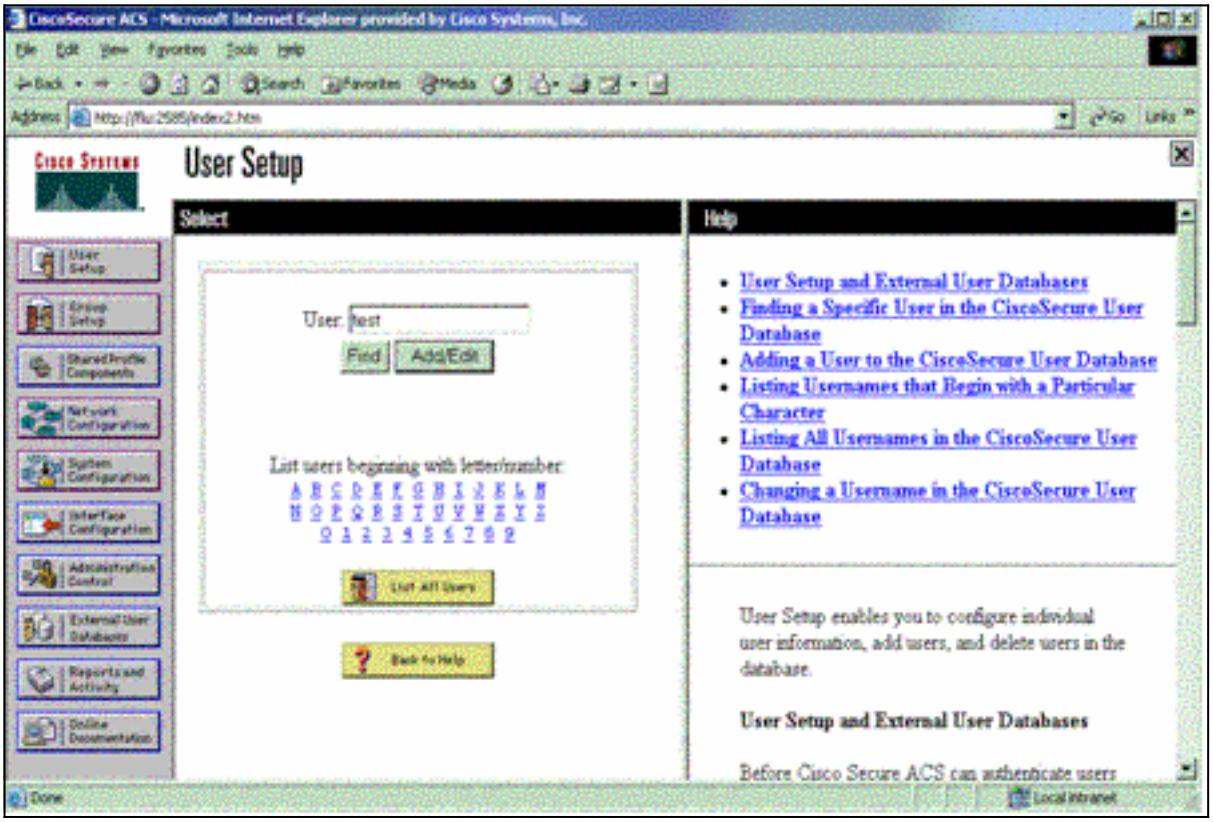
3. **Нажмите Add Запись** для добавления клиента аутентификации, авторизации и учета (AAA)

(NAS). 

4. Введите имя хоста, IP-адрес, и ключ использовал шифровать связь между AAA-сервером и NAS. Выберите **TACACS + (Cisco IOS)** как метод аутентификации. Когда вы будете закончены, нажмите **Submit +Restart** для применения изменений.

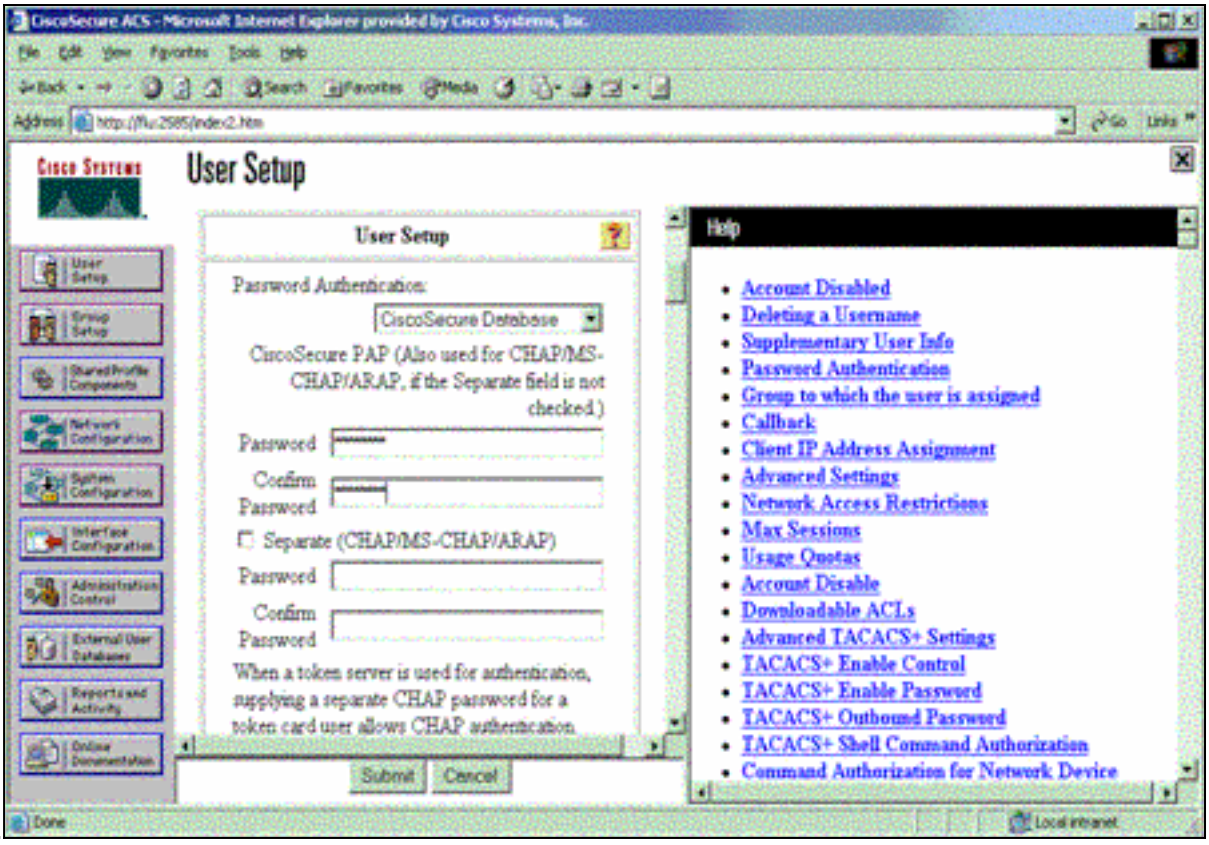


5. Нажмите **User Setup**, введите идентификатор пользователя и нажмите **Add/Edit**.

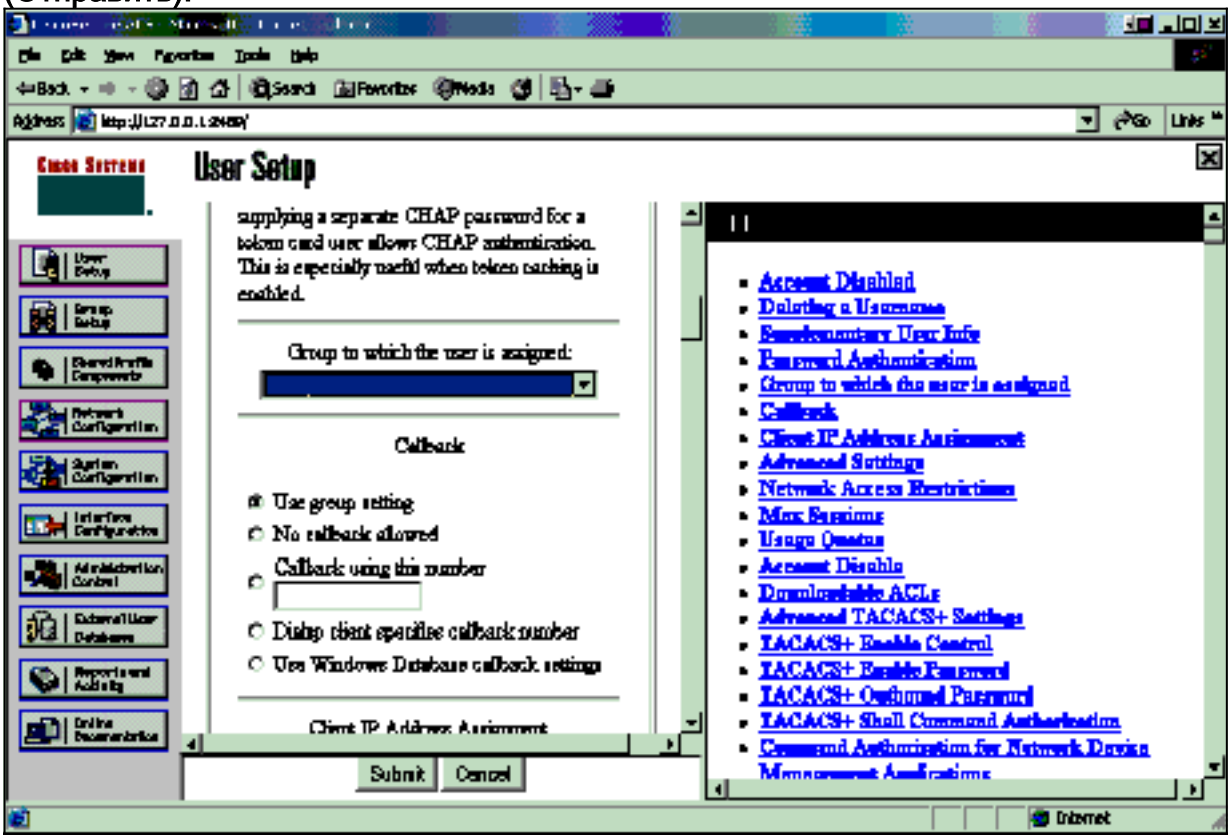


6. Выберите базу данных для аутентификации пользователя. (В данном примере пользователь является "тестом", и внутренняя база данных ACS используется для аутентификации). Введите пароль пользователя и подтвердите

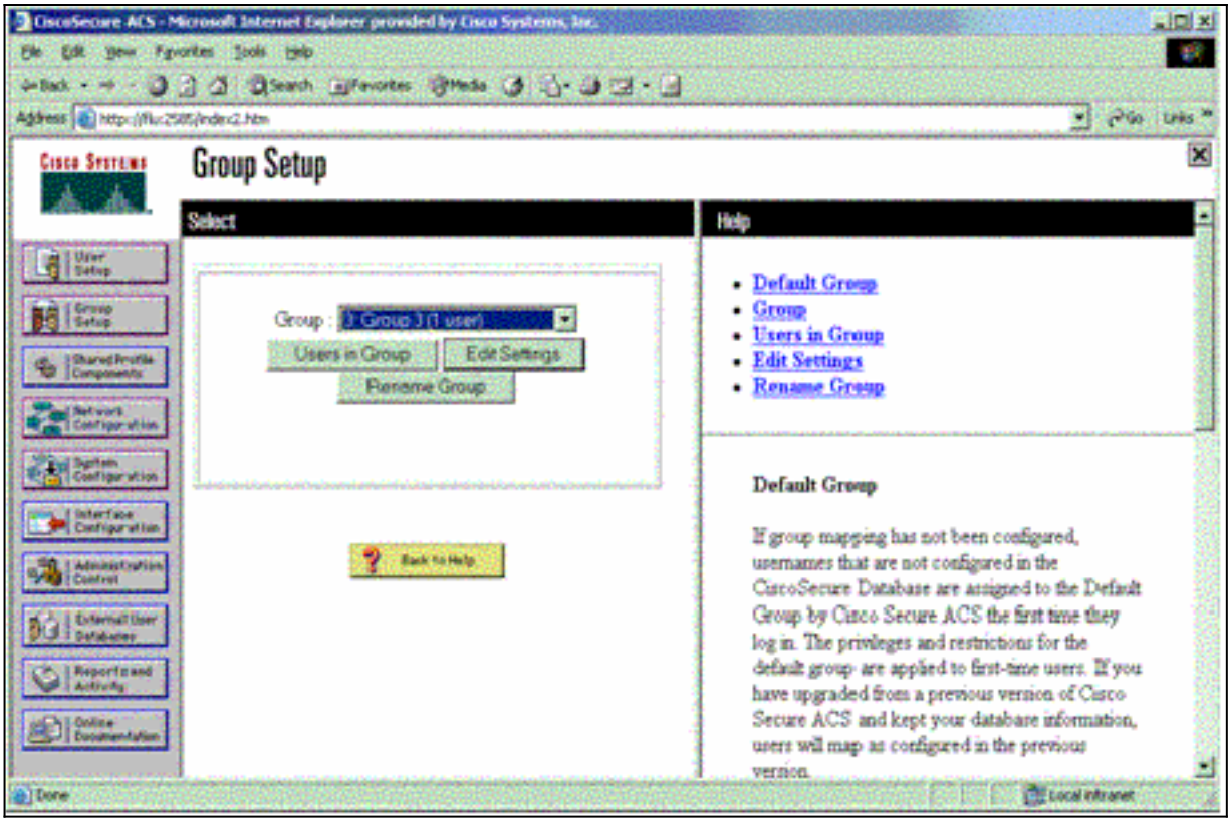
пароль.



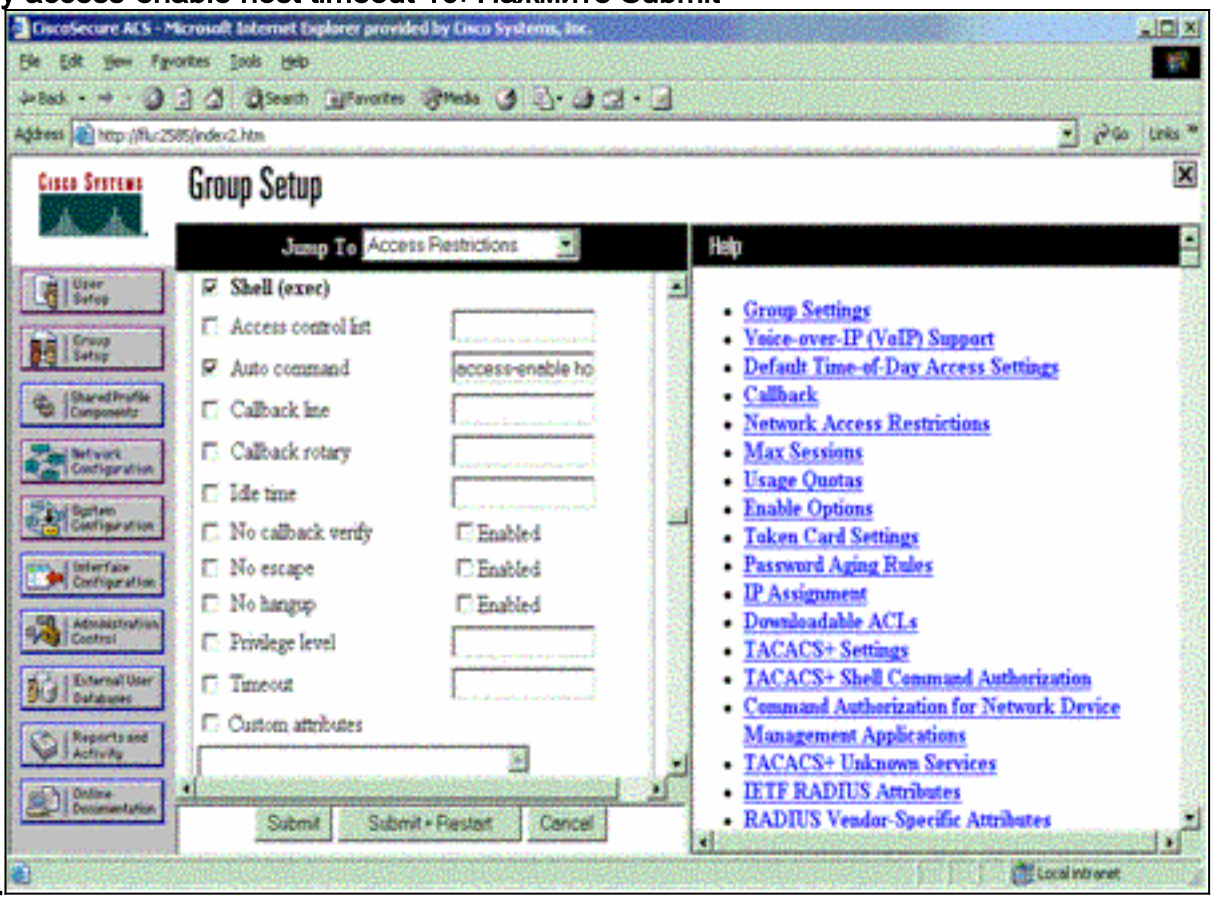
7. Выберите группу, на которую назначают пользователю, и проверьте **параметр группы Использования**. **Нажмите кнопку Submit (Отправить).**



8. **Щелкните на отцию Group Setup.** Выберите группу, на которую пользователю назначили в шаге 7. **Нажмите кнопку Edit Settings (Изменить настройки).**



9. Прокрутите вниз к TACACS + раздел Параметров настройки. **Выберите Shell exec**. Установите флажок для **Команды auto**. Введите auto-command, который будет выполнен на успешную авторизацию пользователя. (Данный пример использует **команду access-enable host timeout 10**. **Нажмите Submit +**



Restart.

TACACS устранения неполадок +

Используйте эти **команды отладки** на NAS для устранения проблем TACACS + проблемы.

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- **аутентификация debug tacacs**? Отображает информацию на TACACS + процесс проверки подлинности. Только доступный в некоторых версиях ПО. Если недоступный, используйте **debug tacacs** только.
- **авторизация debug tacacs**? Отображает информацию на TACACS + процесс авторизации. Только доступный в некоторых версиях ПО. Если недоступный, используйте **debug tacacs** только.
- **события debug tacacs**? Отображает информацию от TACACS + процесс помощника. Только доступный в некоторых версиях ПО. Если недоступный, используйте **debug tacacs** только.

Используйте эти команды для устранения проблем AAA - проблем:

- **debug aaa authentication — отображаются сведения при аутентификации AAA/TACACS+.**
- **debug aaa authorization — отображаются данные авторизации AAA/TACACS+.**

Пример отладочных выходных данных здесь показывает успешную аутентификацию и процесс авторизации на TACACS ACS + сервер.

```
Router#show debug General OS: TACACS+ events debugging is on TACACS+ authentication debugging is
on TACACS+ authorization debugging is on AAA Authentication debugging is on AAA Authorization
debugging is on ========================================================Router#
AAA/BIND(00000009): Bind i/f AAA/AUTHEN/LOGIN (00000009): Pick method list 'default' TPLUS:
Queuing AAA Authentication request 9 for processing TPLUS: processing authentication start
request id 9 TPLUS: Authentication start packet created for 9() TPLUS: Using server 10.48.66.53
TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout TPLUS(00000009)/0/NB_WAIT: socket
event 2 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request TPLUS(00000009)/0/READ: socket
event 1 TPLUS(00000009)/0/READ: Would block while reading TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1 TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/82A2E088: Processing the reply packet TPLUS: Received authen response status
GET_USER (7) TPLUS: Queuing AAA Authentication request 9 for processing TPLUS: processing
authentication continue request id 9 TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout TPLUS(00000009)/0/WRITE: wrote entire 22
bytes request TPLUS(00000009)/0/READ: socket event 1 TPLUS(00000009)/0/READ: read entire 12
header bytes (expect 16 bytes data) TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response TPLUS(00000009)/0/8347F3FC: Processing the
reply packet TPLUS: Received authen response status GET_PASSWORD (8) TPLUS: Queuing AAA
Authentication request 9 for processing TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9 TPLUS(00000009)/0/WRITE/8347EE4C: Started
5 sec timeout TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request TPLUS(00000009)/0/READ:
socket event 1 TPLUS(00000009)/0/READ: read entire 12 header bytes (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1 TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet TPLUS: Received authen response status
PASS (2) AAA/AUTHOR (0x9): Pick method list 'default' TPLUS: Queuing AAA Authorization request 9
for processing TPLUS: processing authorization request id 9 TPLUS: Protocol set to None
.....Skipping TPLUS: Sending AV service=shell TPLUS: Sending AV cmd TPLUS: Authorization request
created for 9(tne-1) TPLUS: using previously set server 10.48.66.53 from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout TPLUS(00000009)/0/NB_WAIT: socket
event 2 TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request TPLUS(00000009)/0/READ: socket
event 1 TPLUS(00000009)/0/READ: Would block while reading TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1 TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet TPLUS: Processed AV autocmd=access-
enable host timeout 10 TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd= AAA/AUTHOR/EXEC(00000009): processing AV
autocmd=access-enable host timeout 10 AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Использование RADIUS

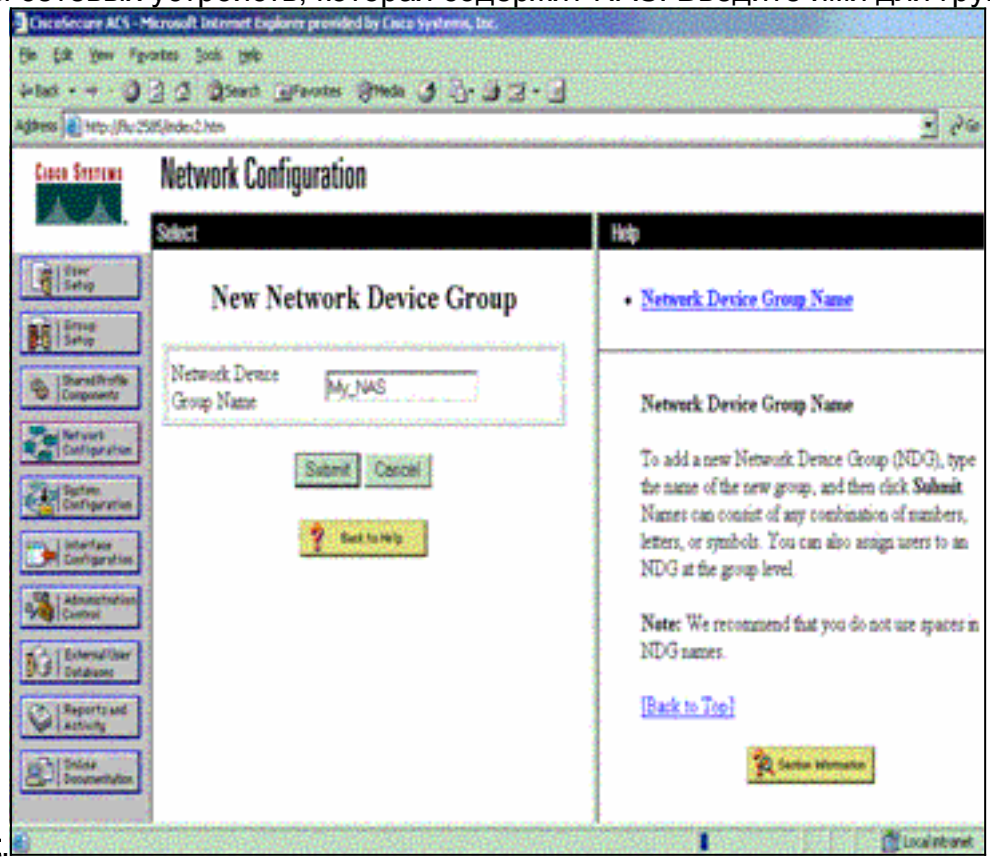
Настройте RADIUS

Для использования RADIUS настройте сервер RADIUS, чтобы вынудить аутентификацию быть сделанной на сервере RADIUS с параметрами авторизации (autocommand), чтобы быть переданной вниз в определяемых производителем характеристика 26, как показано сюда:

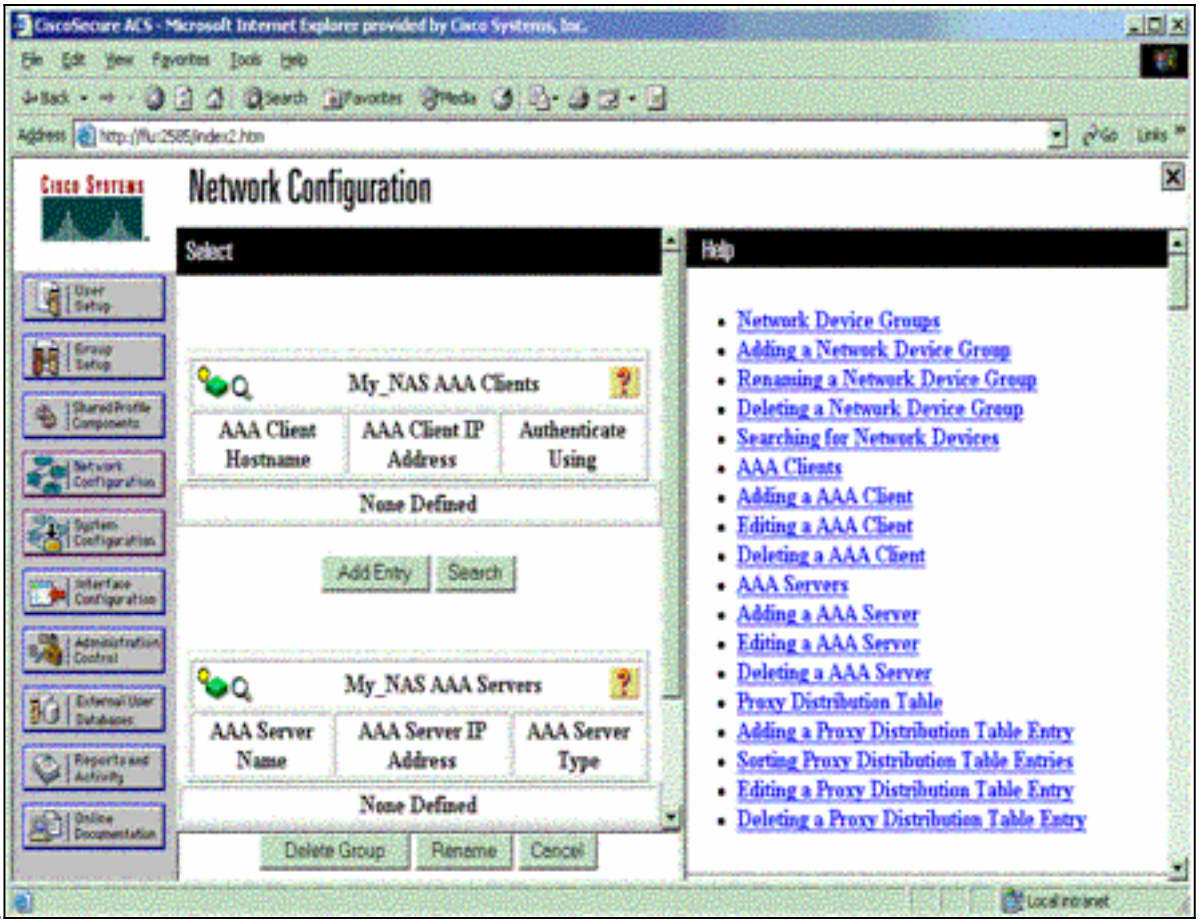
```
aaa new-model!!aaa authentication login default group radius localaaa authorization exec default
group radius localradius-server host 10.48.66.53 auth-port 1645    acct-port 1646 key cisco123
```

Выполните эти шаги для настройки RADIUS на Cisco Secure ACS для Windows:

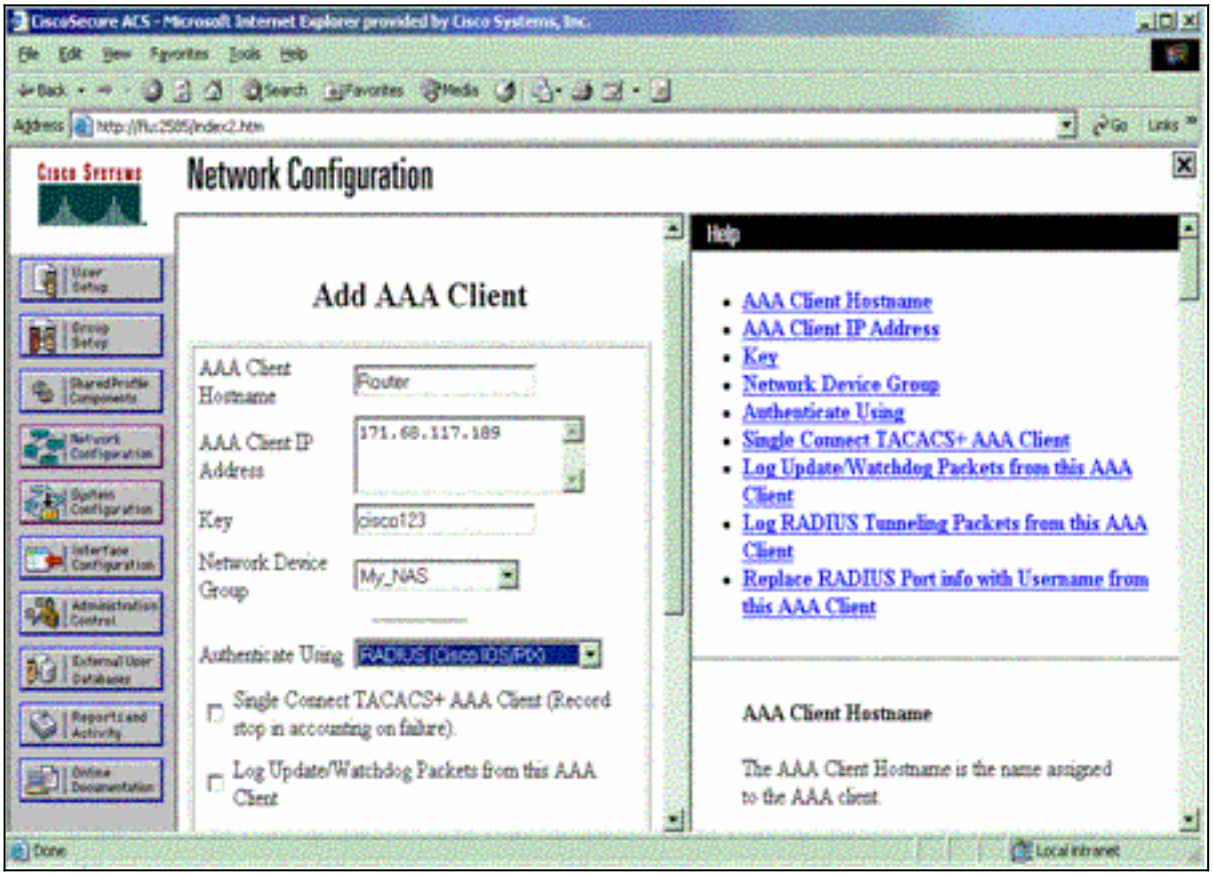
1. Откройте web-браузер и введите адрес вашего сервера ACS, который находится в форме **http://*<IP_address или DNS_name>*:2002**. (Данный пример использует порт по умолчанию 2002.) Входят как admin.
2. **Выберите Network Configuration (Настройка сети). Нажмите Add Запись** для создания Группы сетевых устройств, которая содержит NAS. Введите имя для группы и нажмите **Submit**.



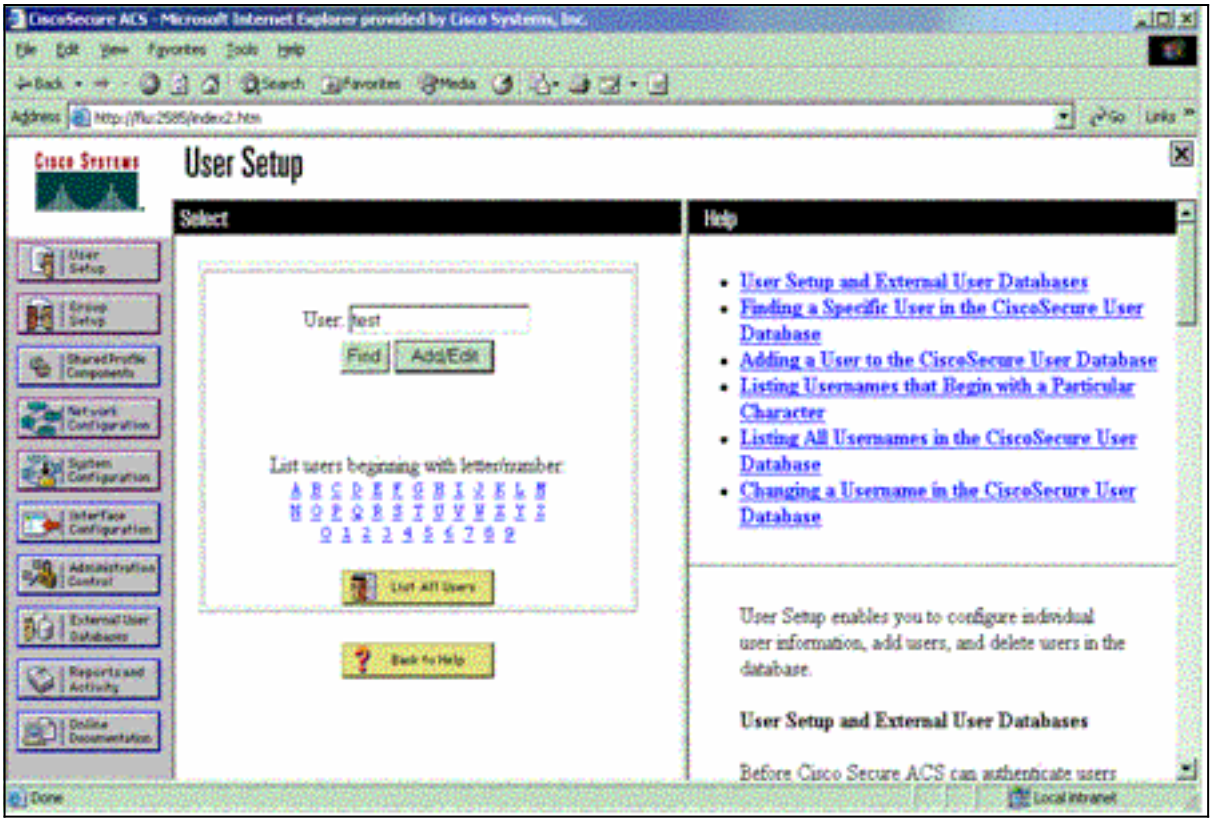
3. **Нажмите Add Запись** для добавления клиента AAA

(NAS). 

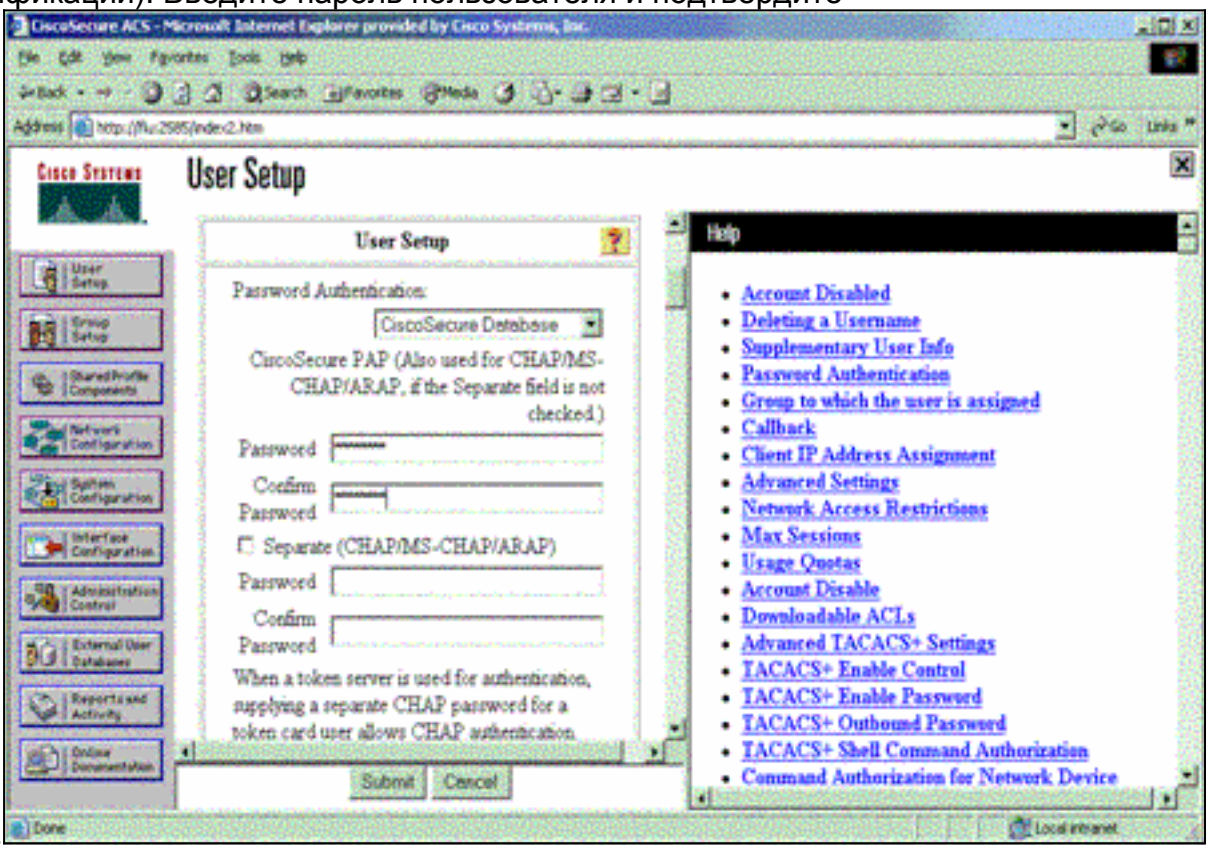
4. Введите имя хоста, IP-адрес, и ключ использовал шифровать связь между AAA-сервером и NAS. Выберите **RADIUS (Cisco IOS / PIX)** как метод аутентификации. Когда вы будете закончены, нажмите **Submit +Restart** для применения изменений.



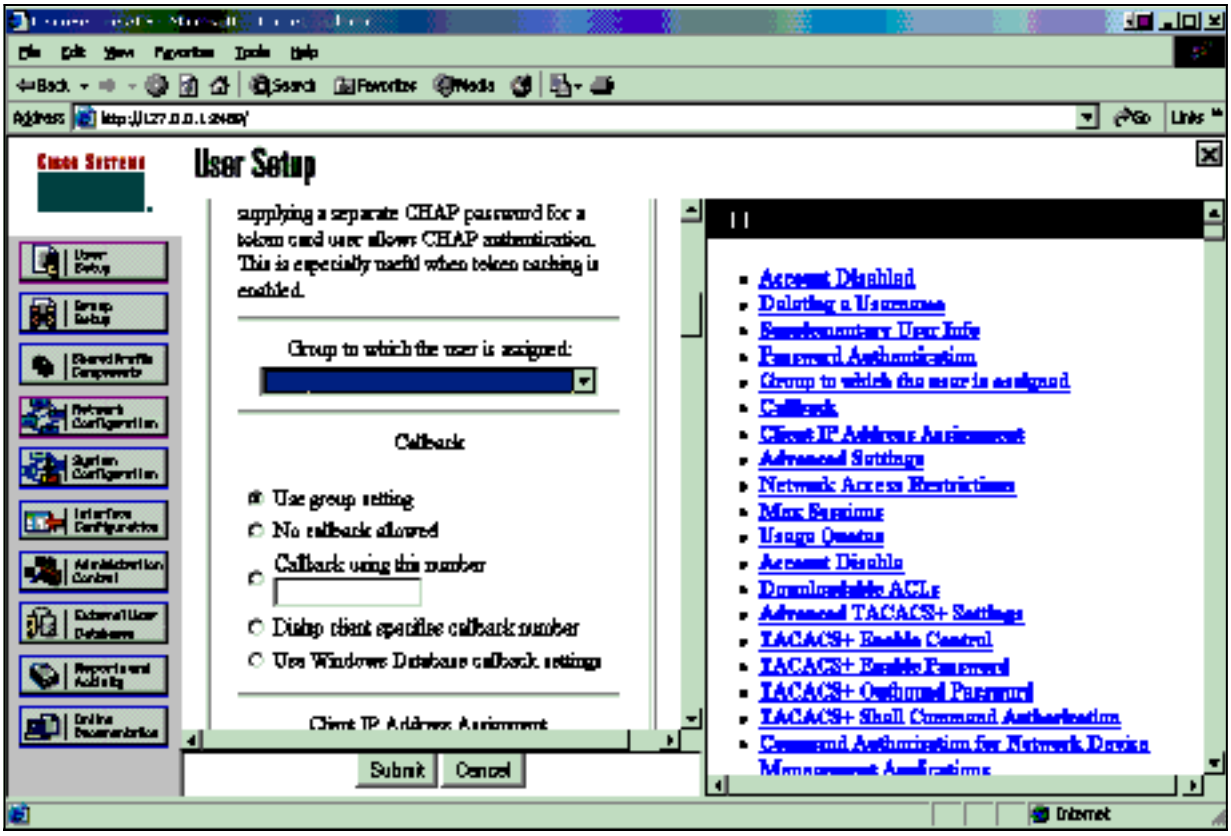
5. Нажмите **User Setup**, введите идентификатор пользователя и нажмите **Add/Edit**.



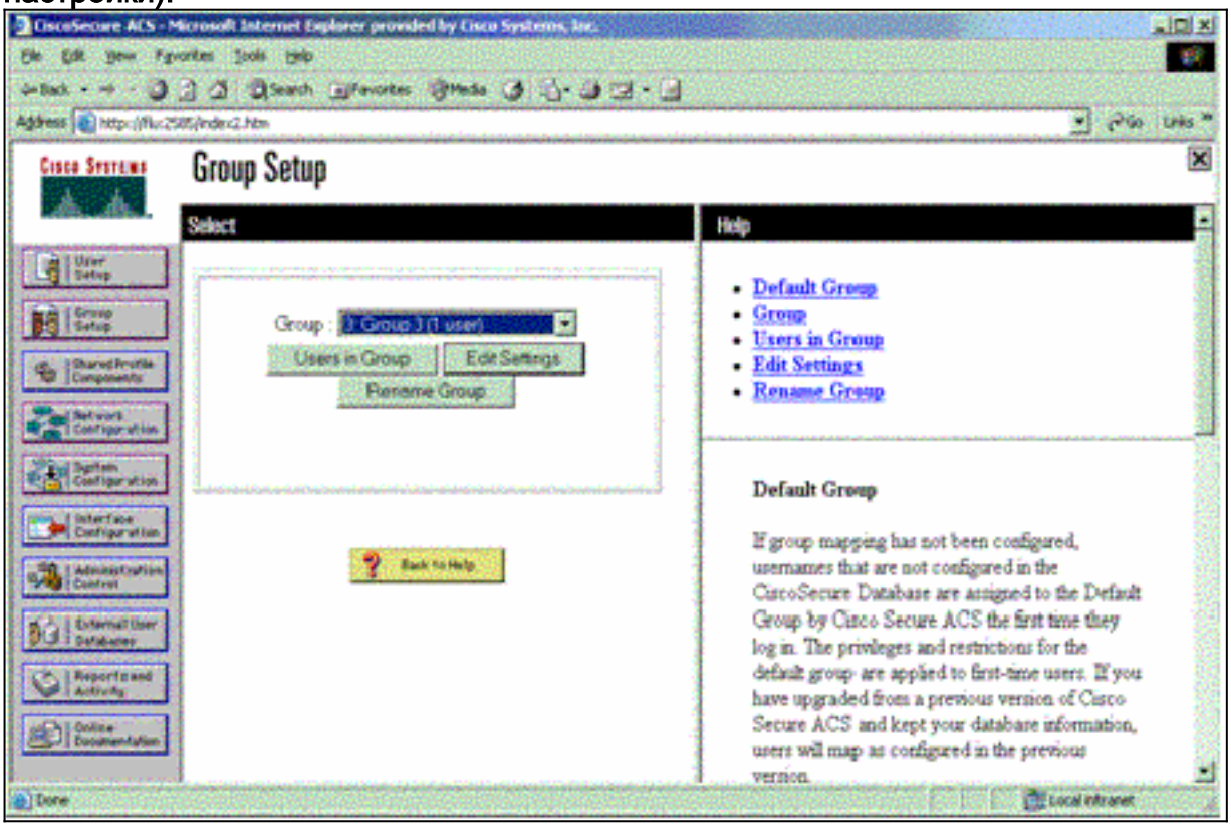
6. Выберите базу данных для аутентификации пользователя. (В данном примере пользователь является "тестом", и внутренняя база данных ACS используется для аутентификации). Введите пароль пользователя и подтвердите пароль.



7. Выберите группу, на которую назначают пользователю, и проверьте **параметр группы Использования**. **Нажмите кнопку Submit (Отправить).**

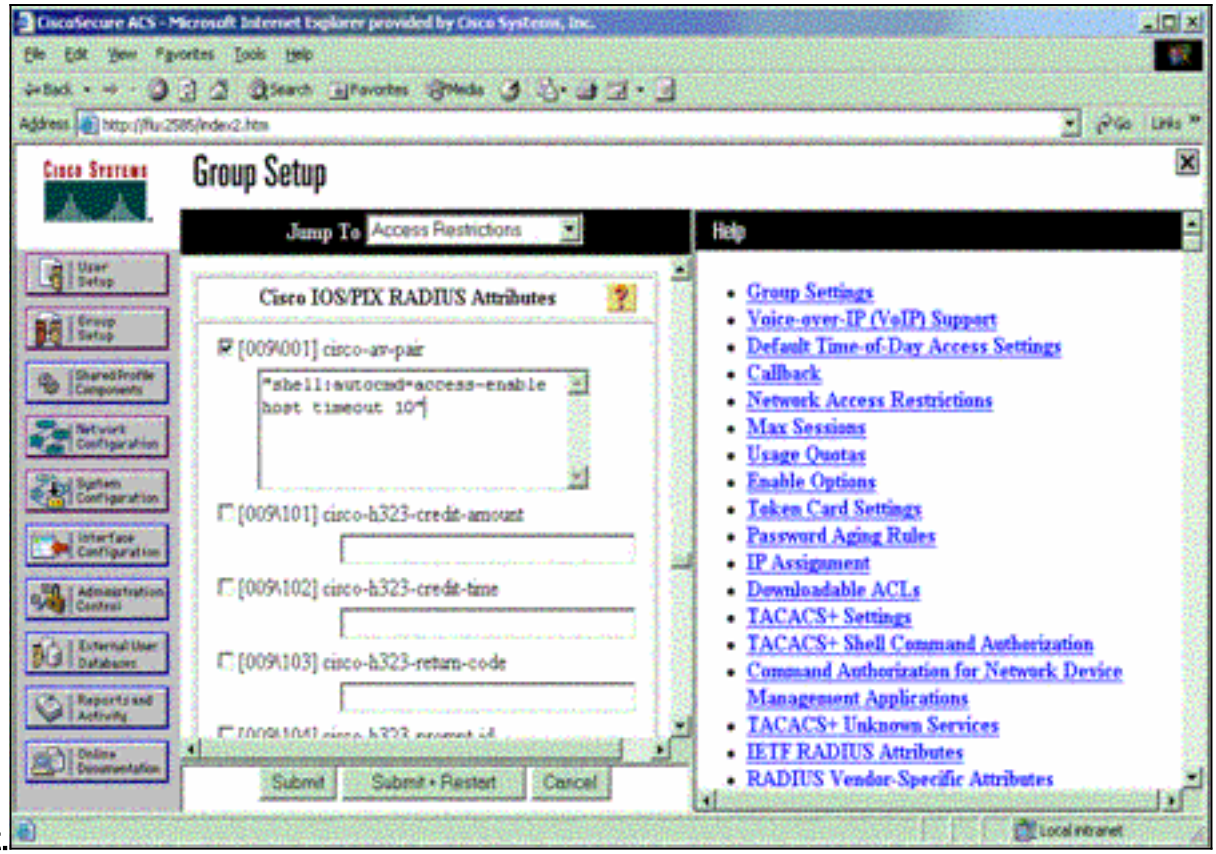


8. Нажмите **Group Setup** и выберите группу, на которую пользователю назначили в предыдущем шаге. **Нажмите кнопку Edit Settings (Изменить настройки).**



9. Прокрутите вниз к Cisco IOS / раздел атрибутов RADIUS PIX. Установите флажок для **Cisco-av-pair**. Введите команду **оболочки**, которая будет выполнена на успешную авторизацию пользователя. (Использование данного примера **shell:autocmd=access-enable размещает таймаут 10. Нажмите Submit +**

Restart.



RADIUS устранения неполадок

Используйте эти **команды отладки** на NAS для устранения проблем Проблем RADIUS.

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- **debug radius – отображает связанную с RADIUS информацию.**

Используйте эти команды для устранения проблем AAA - проблем:

- **debug aaa authentication — отображаются сведения при аутентификации AAA/TACACS+.**
- **debug aaa authorization — отображаются данные авторизации AAA/TACACS+.**

Пример отладочных выходных данных здесь показывает успешную аутентификацию и процесс авторизации на ACS, настроенном для RADIUS.

```
Router#show debug General OS: AAA Authentication debugging is on AAA Authorization debugging is
on Radius protocol debugging is on Radius packet protocol debugging is on
==========================================================Router# AAA/BIND(00000003): Bind i/f
AAA/AUTHEN/LOGIN (00000003): Pick method list 'default' RADIUS/ENCODE(00000003): ask "Username:
" RADIUS/ENCODE(00000003): send packet; GET_USER RADIUS/ENCODE(00000003): ask "Password: "
RADIUS/ENCODE(00000003): send packet; GET_PASSWORD RADIUS: AAA Unsupported [152] 5 RADIUS: 74 74
79 [tty] RADIUS(00000003): Storing nasport 66 in rad_db RADIUS/ENCODE(00000003): dropping
service type, "radius-server attribute 6 on-for-login-auth" is off RADIUS(00000003): Config NAS
IP: 0.0.0.0 RADIUS/ENCODE(00000003): acct_session_id: 1 RADIUS(00000003): sending RADIUS/ENCODE:
Best Local IP-Address 172.18.124.1 for Radius-Server 10.48.66.53 RADIUS(00000003): Send Access-
Request to 10.48.66.53:1645 id 21645/1, len 77 RADIUS: authenticator 5A 95 1F EA A7 94 99 E5 -
BE B5 07 BD E9 05 5B 5D RADIUS: User-Name [1] 7 "test" RADIUS: User-Password [2] 18 * RADIUS:
NAS-Port [5] 6 66 RADIUS: NAS-Port-Type [61] 6 Virtual [5] RADIUS: Calling-Station-Id [31] 14
"171.68.109.158" RADIUS: NAS-IP-Address [4] 6 171.68.117.189 RADIUS: Received from id 21645/1
10.48.66.53:1645, Access-Accept, len 93 RADIUS: authenticator 7C 14 7D CB 33 19 97 19 - 68 4B C3
FC 25 21 47 CD RADIUS: Vendor, Cisco [26] 51 RADIUS: Cisco AVpair [1] 45 "shell:autocmd=access-
enable host timeout 10" RADIUS: Class [25] 22 RADIUS: 43 49 53 43 4F 41 43 53 3A 61 63 31 32 37
```

```
63 30 [CISCOACS:ac127c0] RADIUS: 31 2F 36 36 [1/66] RADIUS(00000003): Received from id 21645/1
AAA/AUTHOR/EXEC(00000003): processing AV autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Дополнительные сведения

- Безопасность замок и ключ Cisco IOS
- Страница поддержки TACACS/TACACS+
- TACACS+ в документации по IOS
- Страница поддержки RADIUS
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация