Содержание

Введение

Этот документ описывает пошаговую процедуру добавляющего Terminal Access Controller Access Control System (TACACS) (TACACS +) сервис проверки подлинности на MGX Cisco 8850/8950/8830 рабочий пересмотр программного обеспечения коммутатора, больше, чем 5.0 с версией 4.2 Access Control Server (ACS) Cisco и выше.

Предварительные условия

Требования

Cisco рекомендует встретить это требования перед попыткой этой конфигурации:

? AAA-сервер достижим от MGX

Используемые компоненты

Этот документ ограничен MGX Cisco 8850/8950/8830 рабочий пересмотр программного обеспечения коммутатора, больше, чем 5.0 и с версией ACS выше 4.2.

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

Примечание: Чтобы получить подробные сведения о командах в данном документе,

используйте Средство поиска команд (только для зарегистрированных клиентов).

Конфигурация на MGX

Пример конфигурации, требуемой на MGX, показывают здесь

Шаг 1. Проверьте версию ПО коммутатора. Вам нужна версия 5.0 или позже настроить TACACS +

```
8950A.7. PXM.a> dspversion
                Основанная версия типа карты типа полки типа образа
  ----------  ----------  ----------   ------------  ------------
                        MGX PXM45 5.1 во время выполнения (20.200)  23
июня 2005, 21:36:08
       Загрузочный                    MGX PXM45 4.0 (0.11) P2  -
```

Шаг 2. Проверьте, что у вас есть правильный IP-адрес:

```
8950A.7. PXM.a> dspifip
   Интерфейсный                    широковещательный Addr подмаски
подсети флага IP Address
   --------------- ---- --------------- --------------- ---------------
            Ethernet/lnPci0 UP 10.66.69.57 255.255.255.128
10.255.255.255
    SLIP/sl0        UP   127.0.0.2       255.0.0.0       (Н/Д)
    ATM/atm0        ,
ВЫКЛЮЧЕННЫЙ 0.0.0.0         0.0.0.0         (Н/Д)
```

Шаг 3. Проверьте, что можно пропинговать сервер ACS: (сервер ACS в 10.106.60.182),

```
8950A.7. PXM.a> пропинговывают 10.106.60.182
PING 10.106.60.182: 56 количеств байтов данных
64 байта от 10.106.60.182: icmp_seq=0. time=250. мс
64 байта от 10.106.60.182: icmp_seq=1. time=240. мс
64 байта от 10.106.60.182: icmp_seq=2. time=240. мс
----10.106.60.182 статистических данных PING----
3 переданные пакета, 3 пакета полученная, 0%-я потеря пакета
распространение в прямом и обратном направлениях (мс) min/avg/Max. =
240/243/250
```

Если эхо-запрос doesn? t проходят, мы должны проверить возможности IP - доступы. Также проверьте **`dspifip`**, и **`bootchange`** настроены с правильным IP-адресом.

```
8950A.7. PXM.a> bootchange

'.' = поле clear; '-' = переходят к предыдущему полю; ^D = выход

загрузочное устройство         : lnPci0
номер процессора    : 0
          host name:
          имя файла:
```

```
inet на ethernet (e): 172.16.157.88>>
inet на объединительной плате (b):
inet хоста (h)       :
inet шлюза (g)    : 172.16.157.1 >>
пользователь (u)            :
пароль FTP (pw) (очищают = rsh использования):
флаги (f)           : 0x0
целевое имя (tn)    :
сценарий (сценарии) запуска  :
другой (o)           :
```

Примечание: Проверьте конфигурацию параметров dspifip, и изменил Основной IP - адрес управления сетью для Взаимодействия через интерфейс IP LAN и адреса ATM как вторичных (использующий **cnfndparm**). Также необходимо настроить bootchange параметры, поместив корректный IP-адрес LAN и шлюз. **routeshow** выходные данные команды должны указать на шлюз по умолчанию для 0.0.0.0 как IP-адрес LAN.

Шаг 4. Проверьте конфигурацию AAA с помощью **dspaaa.** По умолчанию никакой AAA не настроен

```
8950A.7. PXM.a> dspaaa
КОНФИГУРАЦИЯ AAA:
  Методы аутентификации : локальный Cisco
  Методы авторизации  : локальный Cisco
  Тип авторизации     : группа
  Уровень привилегий по умолчанию: NOUSER_GP
  Быстрый Показ         : acs
  Тип сообщения SSH/FTP   : Входящее ИМЯ ДЛЯ ДОСТУПА К ФОРМАТУ ASCII
  Список исключения IOS     :

TACACS + СЕРВЕРЫ:   основной показан сначала

                       Время мертвый сингл
      Порт IP-адреса  время Коннектикут  совместно используемый ключ
шифрования
--------------- ---- --- ---- ------ --------------------------------
----
```

Шаг 5. Настройте IP-адрес AAA-сервера и ключ:

```
8950A.7. PXM.a> tacacs cnfaaa-сервера + - ip 10.66.79.246
Вы хотите изменить ключ шифрования (да/нет)? да
Введите ключ шифрования: Cisco
Повторно введите ключ шифрования: Cisco

TACACS + СЕРВЕРЫ:   основной показан сначала

                       Время мертвый сингл
      Порт IP-адреса  время Коннектикут  совместно используемый ключ
шифрования
--------------- ---- --- ---- ------ --------------------------------
----
```

```
10.66.79.246     49   5   0    истинных  Cisco
```

Шаг 6. Настройка аутентификации:

```
8950A.7. PXM.a> cnfaaa-authen
Синтаксис: cnfaaa-authen <метод> [<метод>...]

       method - {Локальный | по умолчанию | tacacs + | Cisco}
          локальный : Используйте локальную базу данных для
аутентификации.
         по умолчанию: То же как локальный.
         tacacs +: Используйте TACACS + протокол для аутентификации.
         Cisco : Только пользователю маршрута 'Cisco' разрешают войти.
```

Здесь мы делаем TACACS + тогда Локальный и затем Cisco. (Рекомендуется иметь Cisco как последнее прибежище в там?)

```
8950A.7. PXM.a> cnfaaa-authen tacacs + локальный Cisco
КОНФИГУРАЦИЯ AAA:
  Методы аутентификации : tacacs + локальный Cisco
  Методы авторизации  : локальный Cisco
  Тип авторизации     : группа
  Уровень привилегий по умолчанию: NOUSER_GP
  Быстрый Показ         : acs
  Тип сообщения SSH/FTP   : Входящее ИМЯ ДЛЯ ДОСТУПА К ФОРМАТУ ASCII
  Список исключения IOS     :
```

% Warning: Недавно настроенная аутентификация/методы авторизации применяется к новым сеансам. Эта конфигурация не оказывает влияния на существующие сеансы.

Шаг 7. Настройте уровень привилегий по умолчанию, если вы хотите. Мы не настраиваем его в данном примере, т.е. мы оставляем его как по умолчанию:

```
8950A.7. PXM.a> cnfaaa-priv
Синтаксис: cnfaaa-priv <CISCO_GP | SERVICE_GP | SUPER_GP | GROUP1 |
ANYUSER |
                    NOUSER_GP | по умолчанию>
                   Примечание: 'по умолчанию' - то же как NOUSER_GP.)

8950A.7. PXM.a> по умолчанию cnfaaa-priv
КОНФИГУРАЦИЯ AAA:
  Методы аутентификации : tacacs + локальный Cisco
  Методы авторизации  : tacacs + локальный Cisco
  Тип авторизации     : группа
  Уровень привилегий по умолчанию: NOUSER_GP
  Быстрый Показ         : acs
  Тип сообщения SSH/FTP   : Входящее ИМЯ ДЛЯ ДОСТУПА К ФОРМАТУ ASCII
  Список исключения IOS     :
```

Шаг 8. Проверка конфигурации:

```
8950A.7. PXM.a> dspaaa
КОНФИГУРАЦИЯ AAA:
```

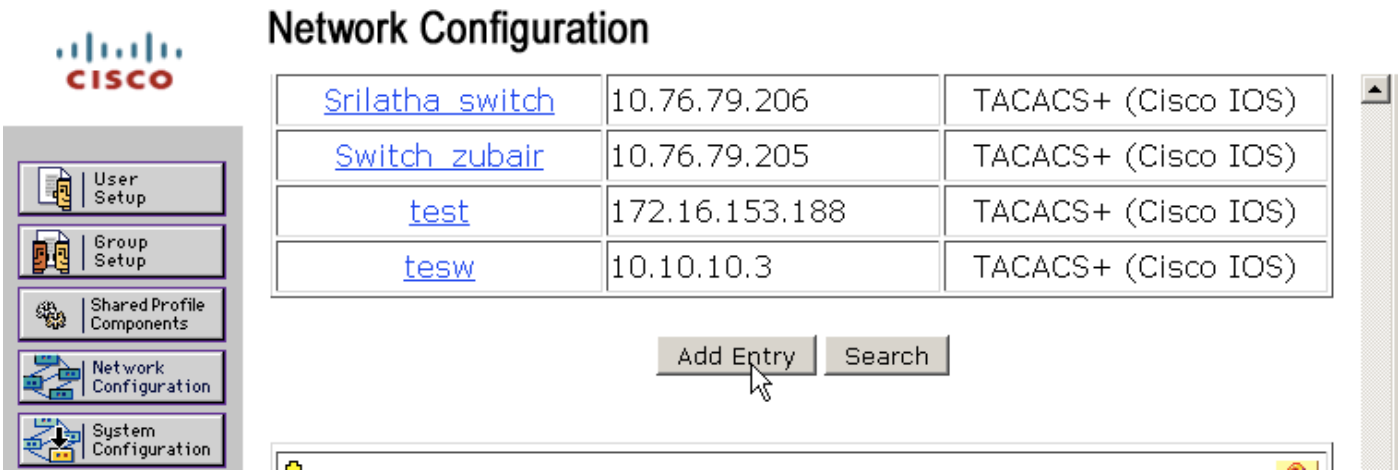
```
  Методы аутентификации : tacacs + локальный Cisco
  Методы авторизации  : tacacs + локальный Cisco
  Тип авторизации     : группа
  Уровень привилегий по умолчанию: NOUSER_GP
  Быстрый Показ          : acs
  Тип сообщения SSH/FTP   : Входящее ИМЯ ДЛЯ ДОСТУПА К ФОРМАТУ ASCII
  Список исключения IOS     :

TACACS + СЕРВЕРЫ:   основной показан сначала

                        Время мертвый сингл
      Порт IP-адреса  время Коннектикут  совместно используемый ключ
шифрования
--------------- ---- --- ---- ------ ---------------------------------
----
10.66.79.246     49   5   0    истинных  Cisco

8950A.7. PXM.a> dspaaa-серверы
TACACS + СЕРВЕРЫ:   основной показан сначала

                        Время мертвый сингл
      Порт IP-адреса  время Коннектикут  совместно используемый ключ
шифрования
--------------- ---- --- ---- ------ ---------------------------------
----
10.66.79.246     49   5   0    истинных  Cisco
```

Конфигурация на ACS

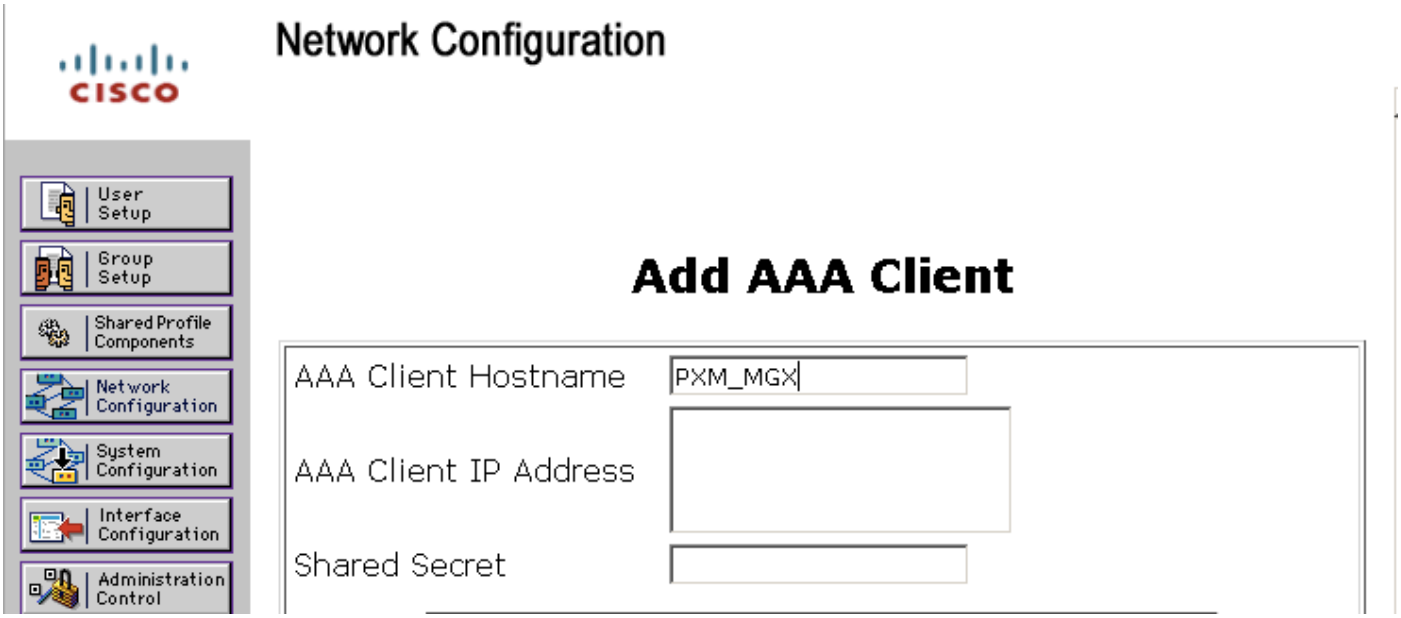
Пример конфигурации, требуемой на ACS, показывают здесь:

Шаг 1. Добавьте MGX как клиента на ACS: (название, используемое здесь, является PXM_MGX, может быть что-либо),

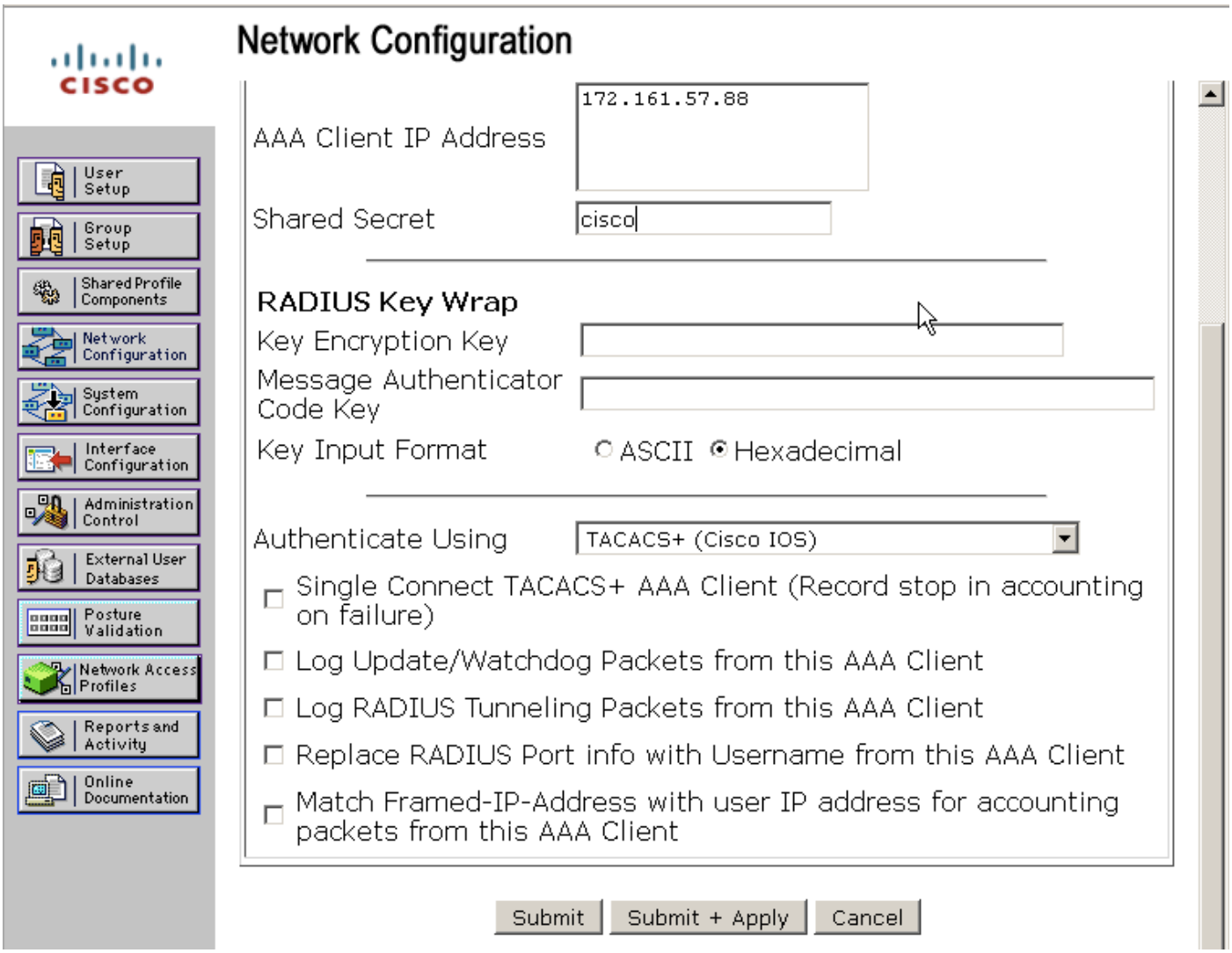
Щелкните **по Network Configuration**
(название, используемое здесь, является PXM_MGX, может быть что-либо),



Шаг 2. Нажмите Add Запись и настройте клиентское имя хоста

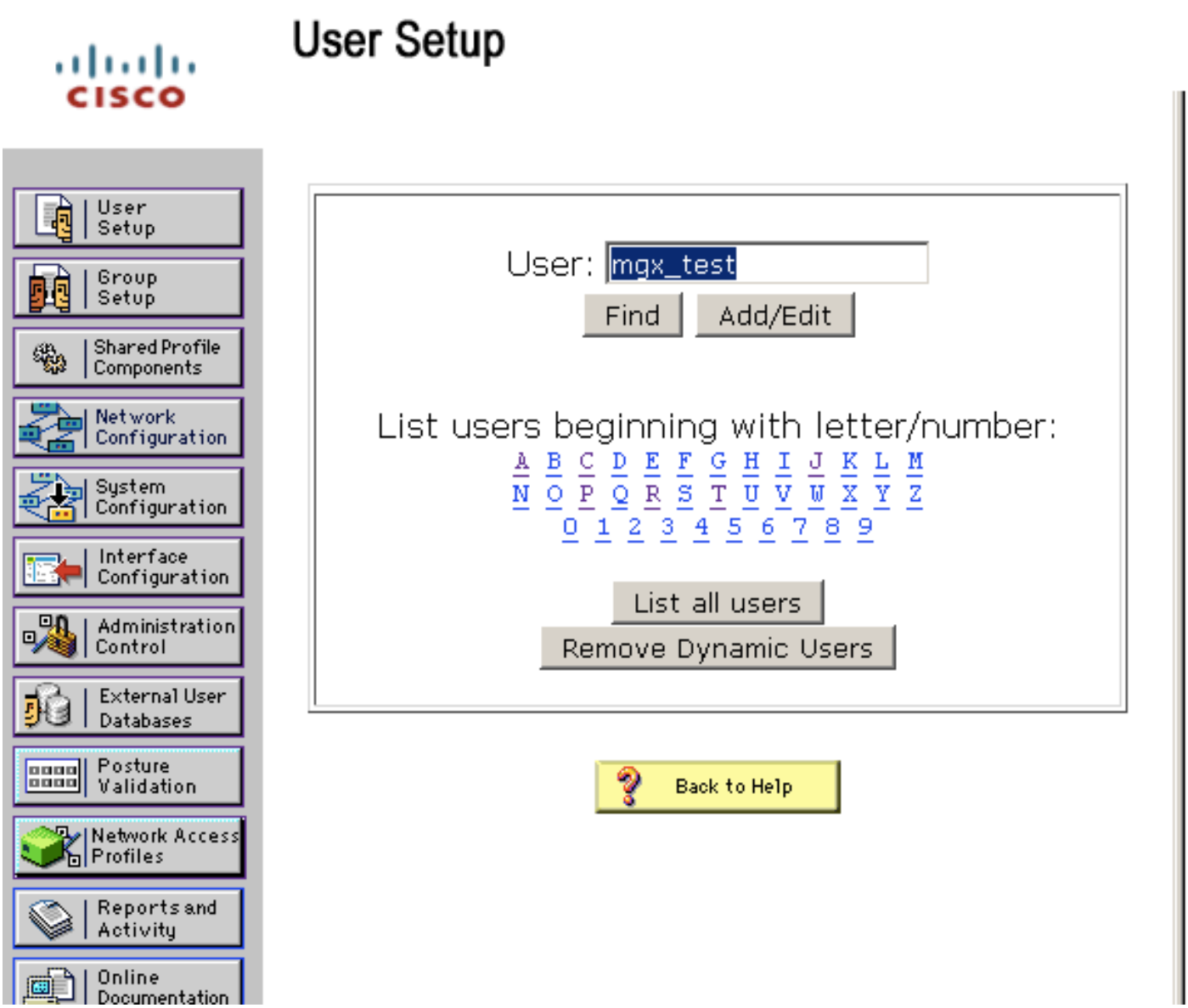


Шаг 3. Настройте IP-адрес клиента AAA (**MGX** в этом случае) и? **ключ**? который должен совпасть с config MGX (ключ, используемый здесь? **Cisco**?).

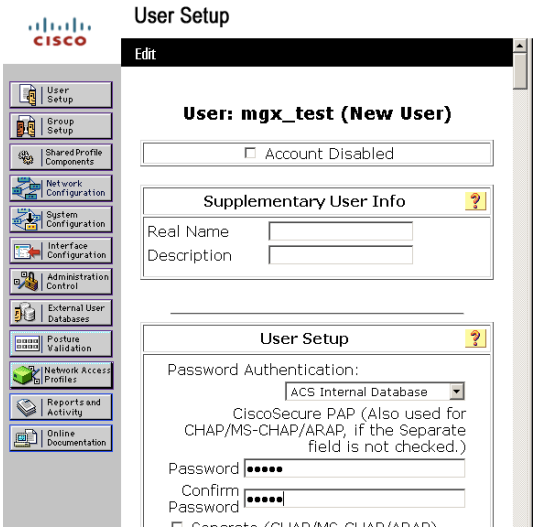


Нажмите кнопку Submit+Apply (Отправить и применить)

Шаг 4. Настройте ПОЛЬЗОВАТЕЛЯ. Щелкните **по User Setup.** Пользователя здесь вызывают? mgx_test?. Нажмите **Add/Edit** после указывания нового имени пользователя

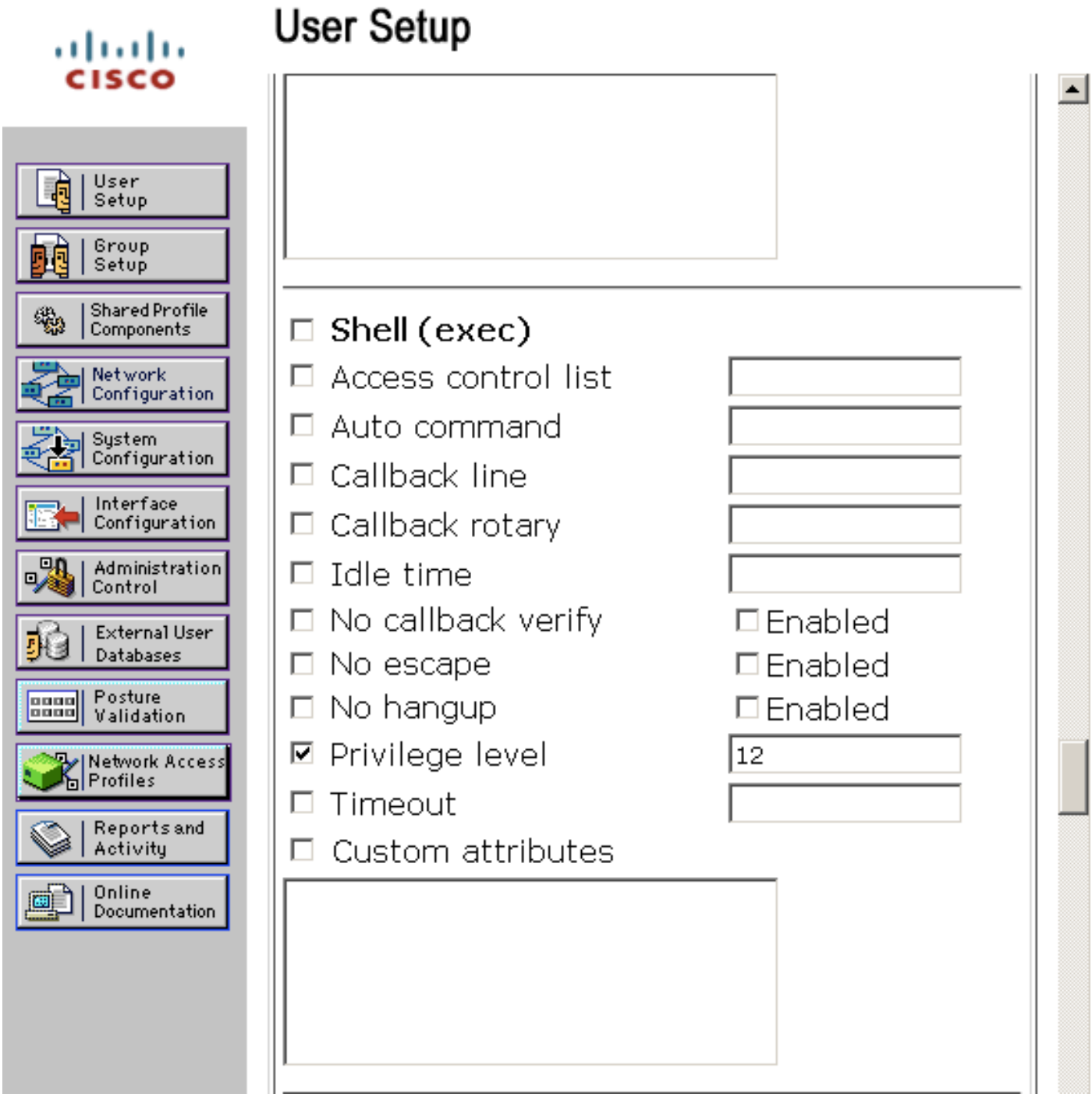


Шаг 5. Настройте пароль для пользователя. Мы настраиваем пароль **"Cisco"** в данном примере



Шаг 6. Установите Уровень привилегий пользователя под **Shell (exec)**. Здесь пользователю дают уровень привилегий 12 или Service_GP.

Примечание: Это - основное различие с аутентификацией IOS. С PXM мы не назначаем, включают привилегию, скорее мы назначаем привилегию shell (exec) на пользователя.



Нажмите **Submit** для фиксации изменений.

Проверка

Telnet к MGX и гарантирует, что пользователь получает уровень привилегий, который мы настроили на сервере ACS (т.е. SERVICE_GP или уровень привилегий 12):

```
telnet % aptcwm02 172.16.157.88
Попытка 172.16.157.88...
Связанный с 172.16.157.88.
Символ выхода является '^]'.
Имя пользователя: mgx_test
Password cisco


8950A.7. PXM.a>, кто

       Слот портов   простаивающий         доступ
UserId    от          запущенного в
-------------------------------------------------------------------------
-------
консоль       7   Cisco 0:00:14          20:55:29 консольного порта
CISCO_GP JUL28
telnet 01 *   7   0:00:00 mgx_test    SERVICE_GP 10.66.69.126   21:04:11
JUL28 <<<
```

Проверьте stats AAA для наблюдения TACACS + опознавательный случай:

```
8950A.7. PXM.a> dspaaa-stats

В последний раз очищенный на: 17:55:42 28.07.2005 (PST)


В последний раз хороший вход в систему authen:     telnet 01
mgx_test   10.66.69.126
                        tacacs +  10.66.79.246/49
                       21:27:34 28.07.2005 (PST)
В последний раз хороший priv группы:         telnet 01
mgx_test   10.66.69.126
                        tacacs +  10.66.79.246/49
                       21:27:34 28.07.2005 (PST)
В последний раз отказавший cmd       : Нет

Введите <CR> для продолжения, Q <CR> для остановки:

____ УРОВЕНЬ КОММУТАТОРА СЧИТАЕТ ____
Метод:                Cisco            локальный            TACACS

# authen сбои:     0                18               0
Сбои автора группы #: 0                0                  0
Сбои автора cmd #: 0                 -----              0
# authen переключается на: 0                 32                 0
Автор # переключается на: 0                1                  0
# authen недостижимый:  -----             ----             0
Недостижимый автор #:  -----             ----             0
# бросает вызов RX:       -----             ----             0
# снабжают дроссели сокетом:    -----             ----             0
# передает TX:                                  ---------9
# передает RX:                                  ---------9
```

```
Вспыхнувшие сообщения #:    -----            ----            0
Передаваемые сообщения прерывания #: -----            ----            0
# поддерживаемый RX AVP:                          ---------2
# неподдерживаемый RX AVP: -----            ----            0
# неизвестный RX AVP:     -----            ----            0

Введите <CR> для продолжения, Q <CR> для остановки:

____ TACACS + УРОВЕНЬ СЕРВЕРА СЧИТАЕТ ____
IP-адрес сервера:     10.66.79.246     0.0.0.0          0.0.0.0
Порт сервера:           49               0               0
# authen сбои:     0               0               0
Сбои автора cmd #: 0               0               0
# authen переключается на: 0               0               0
Автор # переключается на: 0               0               0
# authen недостижимый:  0               0               0
Недостижимый автор #:  0               0               0
# бросает вызов RX:       0               0               0
# передает TX:          9               0               0
# передает RX:          9               0               0
Вспыхнувшие сообщения #:    0               0               0
Передаваемые сообщения прерывания #: 0               0               0
# поддерживаемый RX AVP:   2               0               0
# неподдерживаемый RX AVP: 0               0               0
# неизвестный RX AVP:     0               0               0
Avg задержка ответа:    9               0               0
Задержка ответа Max:    15              0               0
```

Следующие команды отнесены к TACACS на MGX:

```
M7.8. PXM.a>? aaa

   Доступные команды
   -----------------
   cnfaaa-authen
   cnfaaa-автор
   cnfaaa-ftpssh
   cnfaaa-ignore-ios
   cnfaaa-priv
   cnfaaa-приглашение
   cnfaaa-server
   delaaa-server
   dspaaa
   dspaaa-серверы
   dspaaa-stats
   dspaaa-tac-trace
   setaaa-tac-trace
```

Дополнительные сведения

- MGX Cisco 8800/8900 Руководство по конфигурации Программного обеспечения серии, Выпуск 5.4

- Cisco Systems – техническая поддержка и документация