Пример конфигурации мультидоменной аутентификации IEEE 802.1x для коммутаторов Cisco Catalyst уровня 3 с фиксированной конфигурацией

Пример конфигурации мультидоменной аутентификации IEEE 802.1x для коммутаторов Cisco Catalyst уровня 3 с фиксированной конфигурацией

Содержание

Введение

Multi-Domain Authentication (мультидоменная аутентификация) позволяет выполнять аутентификацию IP-телефона и ПК на одном порту коммутатора, располагая их при этом на соответствующих сетях VLAN для передачи голоса и данных. В данном документе описывается способ настройки мультидоменной аутентификации IEEE 802.1x (MDA) для коммутаторов Cisco Catalyst уровня 3 с фиксированной конфигурацией.

Предварительные условия

Требования

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

- Каков принцип работы RADIUS?
- Инструкции по развертыванию коммутатора Catalyst и ACS

- Руководство пользователя для сервера контроля безопасного доступа (ACS) Cisco версии 4.1
- Обзор унифицированного IP-телефона Cisco

Используемые компоненты

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

- Маршрутизатор Cisco серии 3560, использующий программное обеспечение Cisco IOS® версии 12.2(37)SE1

  Примечание. Функция "Multi-Domain Authentication" (мультидоменная аутентификация) поддерживается программным обеспечением Cisco IOS версии 12.2(35)SXF2 и более поздними.
- В данном примере в качестве RADIUS-сервера используется сервер контроля безопасного доступа (ACS) Cisco версии 4.1.

  Примечание. Необходимо определить RADIUS-сервер перед активацией 802.1x на коммутаторе.
- Клиенты ПК, поддерживающие аутентификацию 802.1x

  Примечание. В этом примере используются клиенты Microsoft Windows XP.
- Унифицированный IP-телефон Cisco 7970G с микропрограммным обеспечением SCCP версии 8.2(1)
- Унифицированный IP-телефон Cisco 7961G с микропрограммным обеспечением SCCP версии 8.2(2)
- Сервер объединения средств передачи (MCS; Media Covergence Server) с менеджером унифицированных коммуникаций Cisco (Cisco CallManager) версии 4.1(3)sr2

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, используемые в этом документе, были запущены в исходной (заданной по умолчанию) конфигурации. Если ваша сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Соответствующие продукты

Данные настройки могут использоваться для следующего аппаратного обеспечения:

- Коммутатор Cisco Catalyst серии 3560-E
- Коммутатор Cisco Catalyst серии 3750
- Коммутатор Cisco Catalyst серии 3750-E

Примечание. Коммутатор Cisco Catalyst серии 3550 не поддерживает мультидоменную аутентификацию 802.1x.

Условные обозначения

Дополнительную информацию об используемых в документе обозначениях см. в разделе Условные обозначения, используемые в технической документации Cisco.

Базовые сведения

Стандарт IEEE 802.1x определяет контроль доступа на основе клиент-сервер, а также протокол аутентификации, который препятствует подключению неавторизованных устройств к сети LAN через общедоступные порты. Стандарт 802.1x управляет сетевым доступом с помощью создания для каждого порта двух отдельных виртуальных точек доступа. Одна точка доступа является неуправляемым портом, другая – управляемым. Весь трафик, проходящий через отдельный порт, доступен для каждой из точек доступа. 802.1x аутентифицирует каждое устройство пользователя, подключенное к порту коммутатора, и назначает порт для сети VLAN перед

открытием доступа к службам, предлагаемым коммутатором или сетью LAN. До момента аутентификации устройства 802.1x, средство контроля доступа открывает доступ только для трафика расширяемого протокола аутентификации через LAN (EAPOL), поступающего через порт, к которому подключено устройство. После успешного завершения аутентификации "нормальный" трафик может проходить через порт.

802.1x включает в себя три основных компонента. Каждый из них рассматривается как объект доступа порта (PAE; Port Access Entity).

- Запрашивающее устройство - клиентское устройство, выполняющее запрос на получение сетевого доступа, например, IP-телефоны и присоединенные ПК
- Аутентификатор - сетевое устройство, способствующее выполнению запросов на авторизацию запрашивающего устройства, например, Cisco Catalyst 3560
- Сервер аутентификации - сервер дистанционной аутентификации пользователей по коммутируемым линиям (RADIUS; Remote Authentication Dial-in User Server), выполняющий аутентификацию, например, Cisco Secure Access Control Server (сервер контроля безопасного доступа)

Унифицированные IP-телефоны Cisco также содержат запрашивающее устройство 802.1X. Запрашивающее устройство позволяет сетевым администраторам управлять подключением IP-телефонов к портам коммутатора LAN. Начальная версия запрашивающего устройства 802.1X IP-телефона поддерживает опцию EAP-MD5 для аутентификации 802.1X. При мультидоменной конфигурации, IP-телефон и присоединенный ПК должны независимо выполнить запрос на получение сетевого доступа. Для этого необходимо указать имя пользователя и пароль. Аутентификатор может запросить у RADIUS-сервера информацию, называемую "атрибутами". Атрибуты содержат дополнительную информацию для выполнения авторизации, например, о предоставлении доступа запрашивающему устройству к конкретной сети VLAN. Данные атрибуты могут различаться в зависимости от поставщика. Чтобы передать аутентификатору (Cisco Catalyst 3560) информацию о разрешении запрашивающему устройству (IP-телефону) доступа к голосовой VLAN, компания Cisco использует атрибут RADIUS-сервера `cisco-av-pair`.

Настройка

В этом разделе приводится информация по настройке функции "802.1x multi-domain authentication" (мультидоменная аутентификация 802.1x), описанной в данном документе.

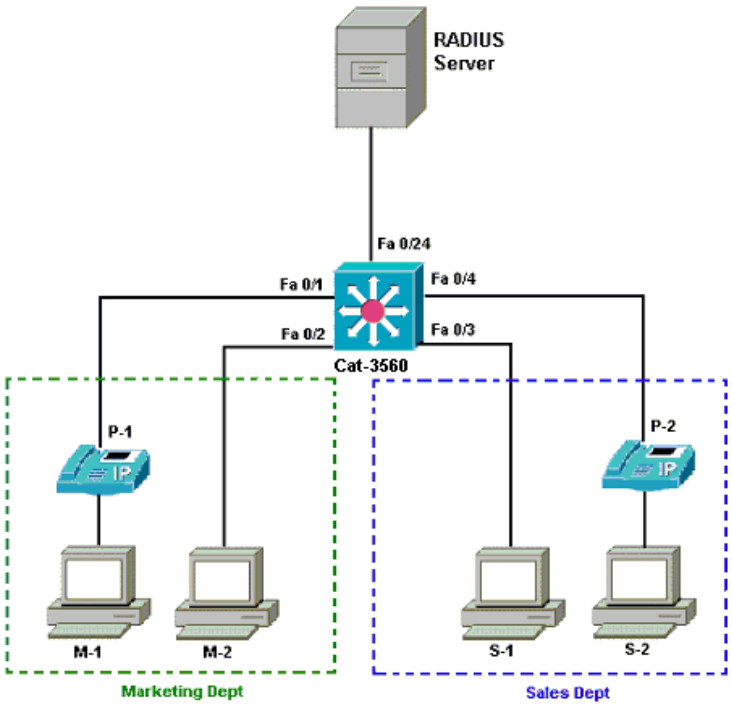
Чтобы настроить конфигурацию, выполните следующие действия:

- Настройка коммутатора Catalyst для мультидоменной аутентификации 802.1x.
- Настройка RADIUS-сервера.
- Настройка клиентов ПК для использования аутентификации стандарта 802.1x.
- Настройка IP-телефонов для использования аутентификации стандарта 802.1x.

Примечание. Дополнительную информацию об используемых в данном документе командах см. в Средстве поиска команд (только для зарегистрированных пользователей).

Схема сети

В данном документе используется следующая схема сети:



- RADIUS-сервер — выполняет фактическую аутентификацию клиента. RADIUS-сервер проверяет подлинность клиента и передает коммутатору решение об авторизации клиента и получении им доступа к сети LAN и службам коммутатора. В данном случае, ACS Cisco установлен и настроен в сервере объединения средств передачи (MCS; Media Covergence Server) для аутентификации и назначения VLAN. Для IP-телефонов сервер MCS также является TFTP-сервером и менеджером унифицированных коммуникаций Cisco (Cisco CallManager).

- Коммутатор - управляет физическим доступом к сети на основе состояния аутентификации клиента. Коммутатор выступает в качестве посредника (прокси) между клиентом и RADIUS-сервером. Он запрашивает у клиента информацию для подтверждения подлинности, сверяет ее с информацией RADIUS-сервера и отправляет ответ клиенту. В данном случае коммутатор Catalyst 3560 также настроен в качестве DHCP-сервера. Поддержка функции аутентификации 802.1x для протокола динамической конфигурации хоста (DHCP) позволяет DHCP-серверу назначать IP-адреса различным классам конечных пользователей. Для этого он добавляет идентификатор аутентифицированного пользователя к процессу обнаружения DHCP. Порты FastEthernet 0/1 и 0/4 являются единственными портами, настроенными для выполнения мульдоменной аутентификации 802.1x. Порты FastEthernet 0/2 и 0/3 по умолчанию установлены в режим подключения одного хоста 802.1x. Порт FastEthernet 0/24 используется для подключения к RADIUS-серверу.

  Примечание. При использовании внешнего DHCP-сервера на интерфейсе SVI (vlan), на котором хранятся данные клиента, необходимо добавлять команду **ip helper-address**, которая указывает на DHCP-сервер.

- Клиенты - это устройства, например, IP-телефоны или рабочие станции, запрашивающие доступ к сети LAN и службам коммутатора и отвечающие на запросы коммутатора. В данном случае клиенты настроены для получения IP-адреса с сервера DHCP. Устройства M-1, M-2, S-1 и S-2 являются рабочими станциями-клиентами, запрашивающими доступ к сети. P-1 и P-2 являются IP-телефонами-клиентами, запрашивающими доступ к сети. M-1, M-2 и P-1 являются клиентскими устройствами в отделе маркетинга. S-1, S-2 и P-2 являются клиентскими устройствами в отделе продаж. IP-телефоны P-1 и P-2 настроены для работы в одной голосовой VLAN (VLAN 3). Рабочие станции M-1 и M-2 настроены для работы в одной VLAN для передачи данных (VLAN 4) после успешного выполнения аутентификации. Рабочие станции S-1 и S-2 также настроены для работы в одной VLAN для передачи данных (VLAN 5) после успешного выполнения аутентификации.

  Примечание. Динамическое назначение сети VLAN с помощью RADIUS-сервера можно использовать только для устройств передачи данных.

Настройка коммутатора Catalyst для мультидоменной аутентификации 802.1x.

В пример настройки коммутатора входит:

- Настройка мультидоменной аутентификации 802.1x на портах коммутатора
- Конфигурация для RADIUS-сервера
- Конфигурация DHCP-сервера для назначения IP-адреса
- Маршрутизация между сетями VLAN для установки соединения между клиентами после выполнения аутентификации

Дополнительную информацию по настройке MDA см. в документе Использование мультидоменной аутентификации.

Примечание. RADIUS-сервер должен всегда подключаться за авторизованным портом.

Примечание. Ниже показана настройка, относящаяся к целям данного документа.

Cat-3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
!--- Установка имени хоста для коммутатора.

Cat-3560(config)#vlan 2
Cat-3560(config-vlan)#name SERVER
Cat-3560(config-vlan)#vlan 3
Cat-3560(config-vlan)#name VOICE
Cat-3560(config-vlan)#vlan 4
Cat-3560(config-vlan)#name MARKETING
Cat-3560(config-vlan)#vlan 5
Cat-3560(config-vlan)#name SALES
Cat-3560(config-vlan)#vlan 6
Cat-3560(config-vlan)#name GUEST_and_AUTHFAIL
!--- Чтобы аутентификация завершилась успешно, VLAN должна уже быть сформирована в коммутаторе.

Cat-3560(config-vlan)#exit
Cat-3560(config)#interface vlan 2
Cat-3560(config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- Адрес шлюза для RADIUS-сервера.

Cat-3560(config-if)#interface vlan 3
Cat-3560(config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- Адрес шлюза для клиентов IP-телефона в VLAN 3.

Cat-3560(config-if)#interface vlan 4
Cat-3560(config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- Адрес шлюза для клиентов PC в VLAN 4.

Cat-3560(config-if)#interface vlan 5
Cat-3560(config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- Адрес шлюза для клиентов PC в VLAN 5.

Cat-3560(config-if)#exit
Cat-3560(config)#ip routing
!--- Активация IP-маршрутизации между VLAN.

Cat-3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#shut
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
!--- Выделенная VLAN для RADIUS-сервера.

Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 , fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
!--- Необходимо настроить голосовую VLAN для IP-телефона, в которой
!--- установлен мультидоменный режим хоста.
!--- Примечание.  При использовании динамической VLAN для назначения голосовой VLAN
!--- на порте коммутатора с активированной функцией MDA голосовое устройство не проходит авторизацию.

Cat-3560(config-if-range)#dot1x port-control auto
!--- Активирование аутентификации IEEE 802.1x на порте.

Cat-3560(config-if-range)#dot1x host-mode multi-domain
!--- Разрешение для хоста и голосового устройства
!--- режима аутентификации на порте, авторизованном в соответствии с IEEE 802.1x.

Cat-3560(config-if-range)#dot1x guest-vlan 6
```

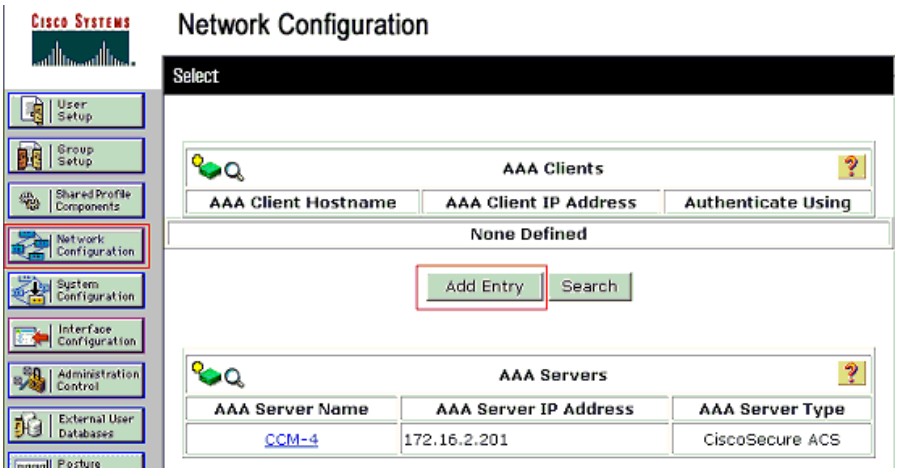
```
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
!--- Функции гостевой VLAN и ограниченной VLAN применимы только
!--- на порте, для которого активирована аутентификация MDA.

Cat-3560(config-if-range)#dot1x reauthentication
!--- Активация периодической повторной аутентификации клиента.

Cat-3560(config-if-range)#dot1x timeout reauth-period 60
!--- Установка количества секунд между попытками повторной аутентификации.

Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
!--- Указание количества разрешенных попыток аутентификации
!--- перед тем, как порт переходит в ограниченную VLAN.

Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
!--- По умолчанию порт, авторизованный в соответствии с 802.1x, позволяет функционировать только с одним клиентом.

Cat-3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- С помощью этого пула назначается IP-адрес для IP-телефонов.
!--- Параметр 150 предназначен для TFTP-сервера.

Cat-3560(dhcp-config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- С помощью этого пула назначается IP-адрес для клиентов PC в отделе маркетинга.

Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
!--- С помощью этого пула назначается IP-адрес для клиентов PC в отделе продаж.

Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1
Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group radius
!---  Должен использоваться стандартный список методов. В противном случае dot1x не работает.

Cat-3560(config)#aaa authorization network default group radius
!--- Чтобы работать с RADIUS, необходима авторизация для назначения динамической VLAN.

Cat-3560(config)#radius-server host 172.16.2.201 key CisCo123
!--- Ключ должен соответствовать ключу, используемому на сервере RADIUS.

Cat-3560(config)#dot1x system-auth-control
!--- Глобальная активация 802.1x.

Cat-3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                Gi0/2
2    SERVER                           active    Fa0/24
3    VOICE                            active    Fa0/1, Fa0/4
4    MARKETING                        active
5    SALES                            active
6    GUEST_and_AUTHFAIL               active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Примечание. См. дополнительные сведения о командах, используемых в данном документе, в Средстве поиска команд (только для зарегистрированных пользователей).

Настройка RADIUS-сервера

RADIUS-серверу назначается статический IP-адрес 172.16.2.201/24. Выполните следующие действия, чтобы настроить RADIUS-сервер для клиента AAA:

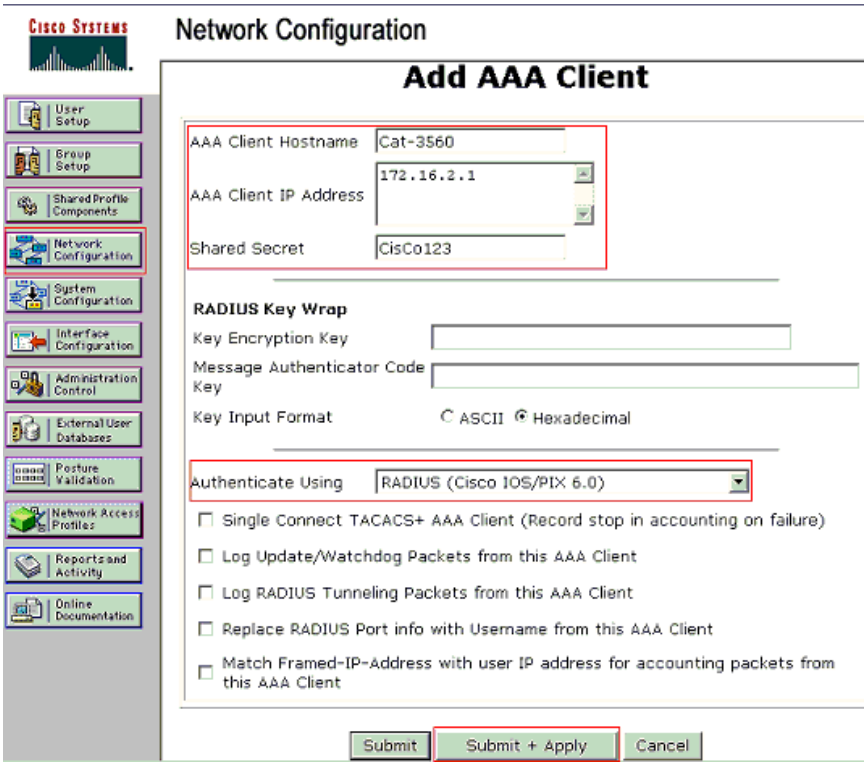
1. Нажмите **Network Configuration** в окне управления ACS для настройки AAA-клиента.
2. Нажмите **Add Entry** в разделе клиентов AAA.



3. Определите для AAA-клиента имя хоста, IP-адрес, общий секретный ключ и тип аутентификации следующим образом:
   - Имя хоста AAA-клиента = имя хоста коммутатора (**Cat-3560**).
   - IP-адрес AAA-клиента = IP-адрес интерфейса управления коммутатором (**172.16.2.1**).
   - Общий секретный ключ = настроенный ключ RADIUS на коммутаторе (**CisCo123**).

     Примечание. Для нормальной работы, клиент AAA и ACS должны иметь одинаковый общий секретный ключ. При использовании ключей необходимо учитывать регистр.
   - Используемая аутентификация = **RADIUS (Cisco IOS/PIX 6.0)**.

     Примечание. Доступ к паре атрибут-значение (AV) Cisco можно получить с помощью этого параметра.
4. Нажмите **Submit + Apply**, чтобы изменения вступили в силу (см. пример):

4. 

Настройка группы

Используйте приведенную таблицу, чтобы настроить RADIUS-сервер для аутентификации.

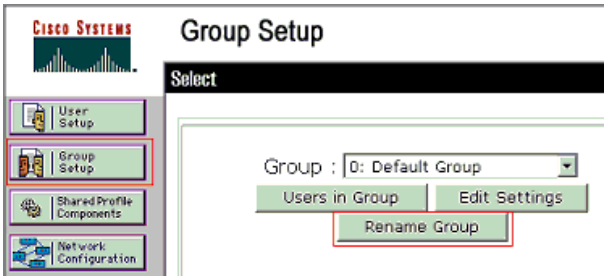
Устройство	Отдел	Группа	Пользователь	Пароль	Виртуальная локальная сеть	DHCP-пул
M-1	Маркетинг	Маркетинг	Менеджер отдела маркетинга	MMcisco	MARKETING	Маркетинг
M-2	Маркетинг	Маркетинг	Сотрудники отдела маркетинга	MScisco	MARKETING	Маркетинг
S-2	Отдел продаж	Отдел продаж	Менеджер отдела продаж	SMcisco	SALES	Отдел продаж
S-1	Отдел продаж	Отдел продаж	Сотрудники отдела продаж	SScisco	SALES	Отдел продаж
P-1	Маркетинг	IP-телефоны	CP-7970G-SEP001759E7492C	P1cisco	VOICE	IP-телефоны
P-2	Отдел продаж	IP-телефоны	CP-7961G-SEP001A2F80381F	P2cisco	VOICE	IP-телефоны

Создайте группы для подключения к виртуальной локальной сети 3 (VOICE), 4 (MARKETING) и 5 (SALES). В данном случае для этой

цели были созданы группы **IP Phones** (IP-телефоны), **Marketing** (Маркетинг) и **Sales** (Отдел продаж).

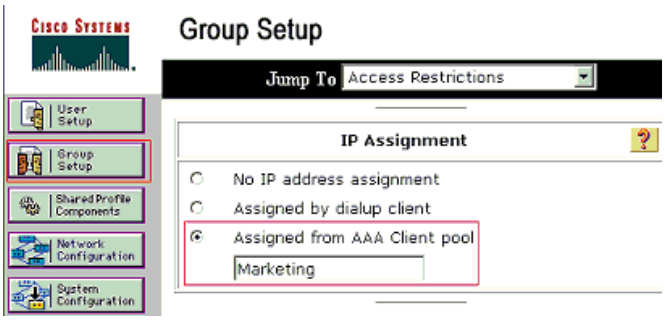
Примечание. Это настройка групп **Marketing** и **IP Phones**. Для конфигурации группы **Sales** выполните следующие действия для группы **Marketing**.

1. Чтобы создать группу выберите **Group Setup** и измените имя группы, установленное по умолчанию.



2. Чтобы настроить группу, выберите группу из списка и нажмите **Edit Settings**.

3. Определите назначение IP-адреса клиента как **Assigned by AAA client pool** (назначенный из пула клиентов AAA-сервера). Ведите имя пула IP-адресов, настроенного на коммутаторе для этой группы клиентов.



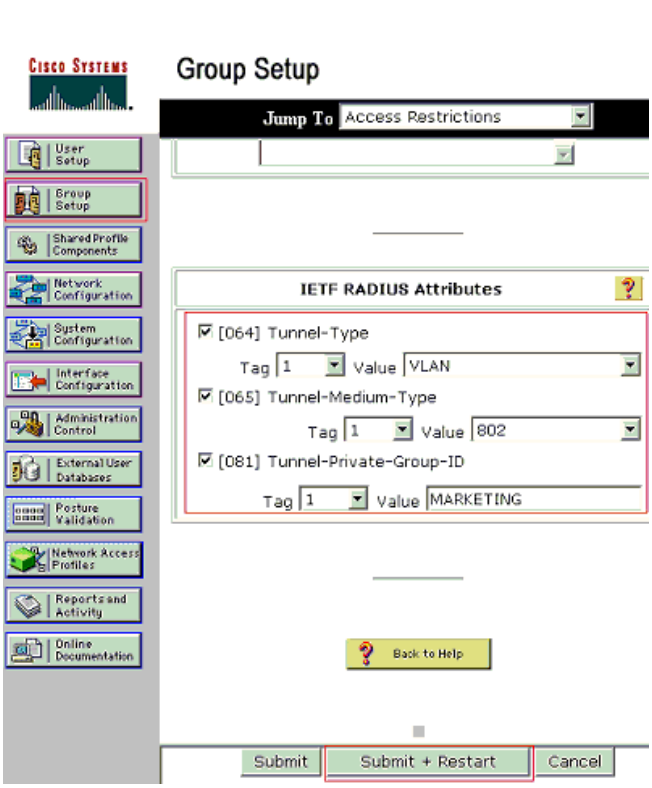
Примечание. Выбирайте этот параметр и вводите название IP-пула клиентов AAA в соответствующем поле только тогда, когда пользователь должен получить IP-адрес, назначенный из пула IP-адресов, настроенного на AAA-сервере.

Примечание. Для настройки только группы **IP Phones** пропустите следующий шаг (4) и переходите к шагу 5.

4. Определите атрибуты Группы поддержки сети Интернет (IETF) **64**, **65** и **81**, а затем нажмите **Submit + Restart**.

   Убедитесь, что теги значений установлены в **1**, как показано в этом примере. Catalyst игнорирует любой тег, кроме 1. Чтобы назначить пользователя конкретной VLAN, необходимо также определить атрибут **81** с соответствующим *именем* или *номером* VLAN.

   Примечание. В случае использования *имени* VLAN оно должно точно соответствовать имени, заданному на коммутаторе.



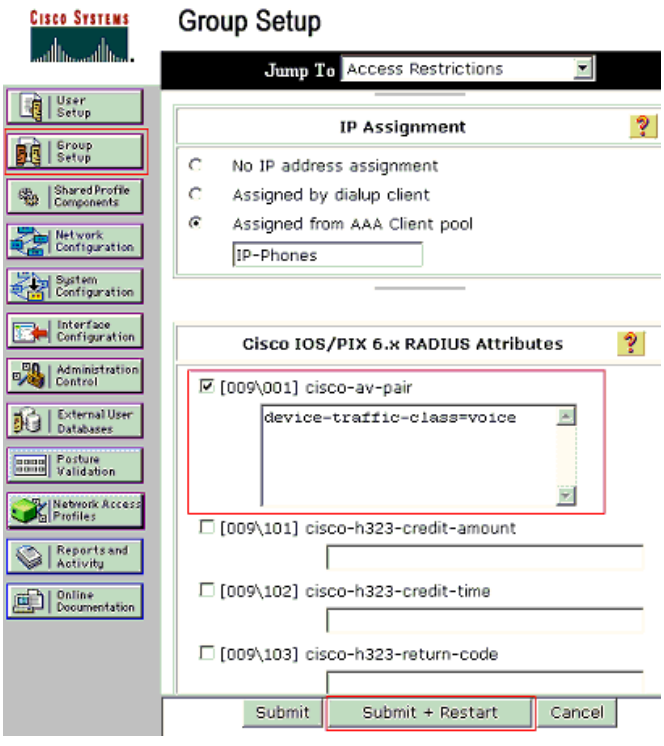
Примечание. Дополнительные сведения по данным атрибутам IETF см. в RFC 2868: атрибуты RADIUS для поддержки протокола туннеля.

Примечание. В исходной конфигурации ACS-сервера атрибуты RADIUS IETF могут не отображаться в **User Setup**. Чтобы активировать атрибуты IETF на экранах конфигурации пользователя, выберите **Interface configuration > RADIUS (IETF)**. Затем выполните проверку атрибутов **64**, **65** и **81** в столбцах User и Group.

Примечание. Если атрибут **81** IETF не определен и порт является портом коммутатора в режиме доступа, клиент назначается на VLAN доступа на порту. Если для динамической VLAN был назначен атрибут **81**, а порт – это порт коммутатора в режиме доступа, необходимо ввести команду **aaa authorization network default group radius** на коммутаторе. С помощью этой команды будет назначен порт для VLAN, который предоставляет RADIUS-сервер В противном случае 802.1x переключит порт в состояние `AUTHORIZED` (авторизован) после аутентификации пользователя. Однако порт по прежнему будет находиться во VLAN порта по умолчанию и соединение не состоится.

Примечание. Следующее действие применимо только к группе **IP Phones**.

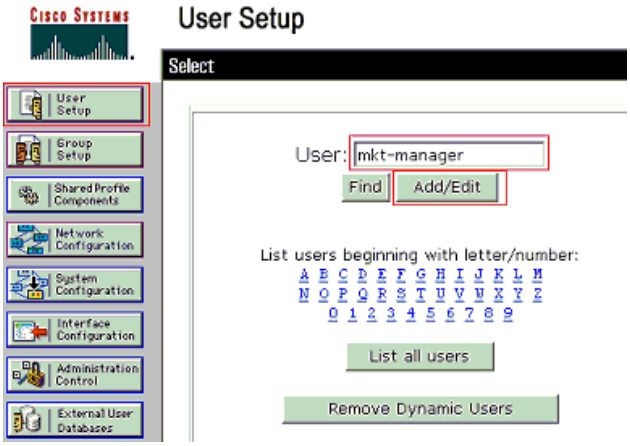
5. Настройте RADIUS-сервер на отправку пары атрибут-значение (AV) Cisco для авторизации голосового устройства. Без этого коммутатор распознает голосовое устройство как устройство данных. Определите паре атрибут-значение (AV) Cisco значение *device-traffic-class=voice*, а затем нажмите **Submit + Restart**.



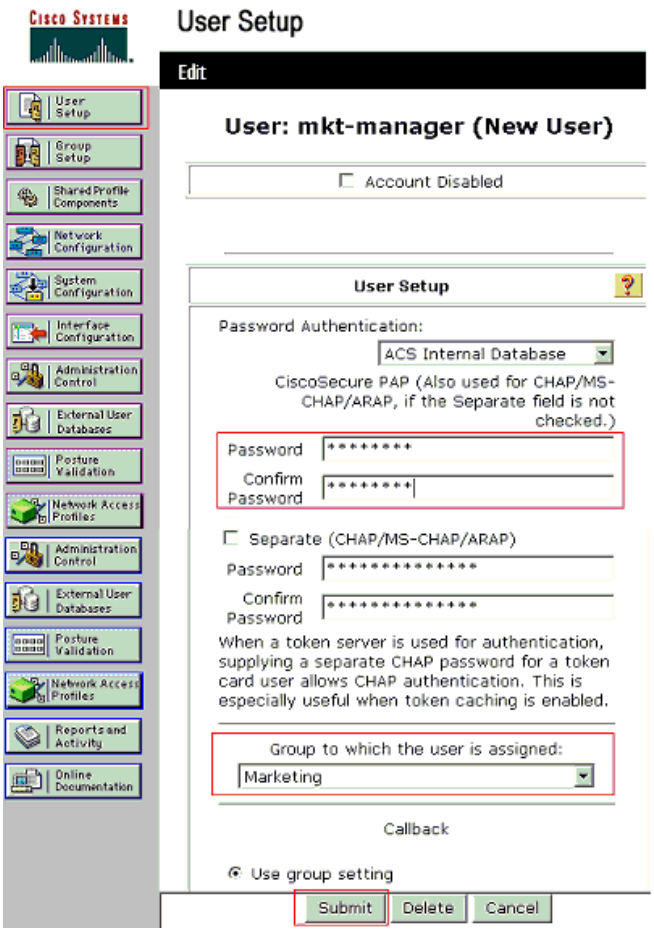
Настройки пользователя

Чтобы добавить и настроить пользователя, выполните следующие действия.

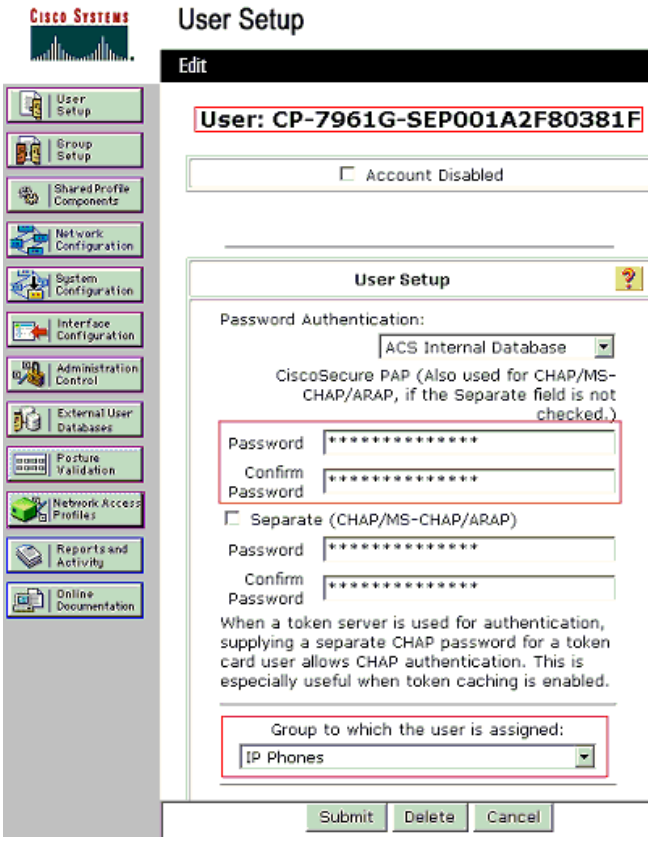
1. Чтобы добавить и настроить пользователя, выберите **User Setup**. Введите имя пользователя и нажмите **Add/Edit**.



2. Укажите имя пользователя, пароль и группу для этого пользователя.



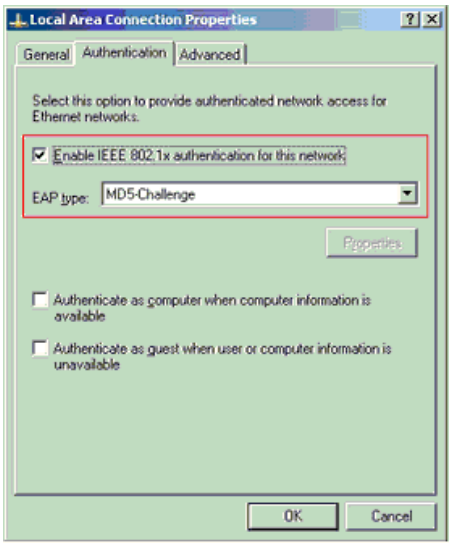
3. IP-телефон использует идентификатор устройства в качестве имени пользователя и общий секретный ключ в качестве пароля для аутентификации. Эти значения должны соответствовать значениям на сервере RADIUS. IP-телефоны P-1 и P-2 создают имена пользователей, которые совпадают с идентификатором устройства и имена пользователей, которые совпадают с общим секретным ключом. Дополнительные сведения по идентификатору устройств и общему секретному ключу IP-телефона см. в разделе Настройка IP-телефонов для использования аутентификации по стандарту 802.1x.

3. 

Настройка клиентов ПК для использования аутентификации по стандарту 802.1x

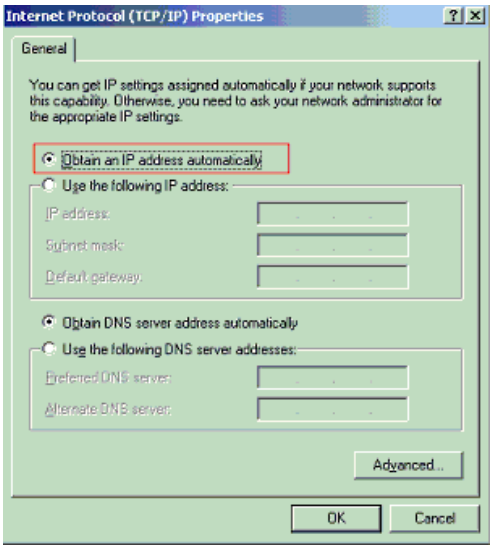
Этот пример относится исключительно к клиенту Расширяемого протокола аутентификации (EAP) Microsoft Windows XP через LAN (EAPOL):

1. Выберите **Start > Control Panel > Network Connections**, а затем нажмите правой кнопкой мыши **Local Area Connection** и выберите **Properties**.
2. Убедитесь, что на вкладке General установлен параметр **Show icon in notification area when connected** (при подключении показывать значок в области уведомлений).
3. На вкладке Authentication установите **Enable IEEE 802.1x authentication for this network** (включить аутентификацию IEEE 802.1x для этой сети).
4. Установите тип EAP: **MD5-Challenge** (см. пример):



Для настройки клиентов на получение IP-адреса с сервера DHCP, выполните следующие действия.

1. Выберите **Start > Control Panel > Network Connections**, а затем нажмите правой кнопкой мыши **Local Area Connection** и выберите **Properties**.
2. На вкладке General нажмите **Internet Protocol (TCP/IP)**, а затем – **Properties**.
3. Выберите **Obtain an IP address automatically** (получать IP-адрес автоматически).



Настройка IP-телефонов для использования аутентификации по стандарту 802.1x

Чтобы настроить IP-телефоны для аутентификации по стандарту 802.1x, выполните следующие действия.

1. Нажмите кнопку **Settings**, чтобы получить доступ к параметрам **802.1X Authentication** (аутентификация по стандарту 802.1X), выберите **Security Configuration > 802.1X Authentication > Device Authentication**.
2. Установите значение **Enabled** для параметра **Device Authentication**.
3. Нажмите функциональную клавишу **Save**.
4. Выберите **802.1X Authentication > EAP-MD5 > Shared Secret** для установки пароля телефона.
5. Введите общий секретный ключ и нажмите **Save**.

   Примечание. Пароль должен иметь длину 6-32 символа и состоять из любого сочетания цифр и букв. Если это условие не соблюдается, отобразится сообщение `That key is not active here` (этот ключ недействителен здесь), а пароль не будет сохранен.

   Примечание. При отключении аутентификации по стандарту 802.1X или при возникновении необходимости восстановить заводские параметры по умолчанию на телефоне ранее установленный общий ключ MD5 удаляется.

   Примечание. Другие параметры, такие как идентификатор устройства и именованная область (Realm), не подлежат настройке. Идентификатор устройства используется в качестве имени пользователя для аутентификации по стандарту 802.1x. Идентификатор формируется из номера модели телефона и уникального MAC-адреса. Он отображается в следующем формате: CP-<модель>-SEP-<MAC-адрес>. Например, **CP-7970G-SEP001759E7492C**. Дополнительные сведения см. в разделе Параметры аутентификации по стандарту 802.1X.

Для настройки IP-телефона на получение IP-адреса с сервера DHCP, выполните следующие действия.

1. Нажмите кнопку **Settings**, чтобы получить доступ к разделу **Network Configuration** и выберите **Network Configuration**.
2. Разблокируйте параметры **Network Configuration**. Чтобы разблокировать, нажмите **#.

   Примечание. Не пытайтесь разблокировать параметры с помощью **#, а затем сразу же заблокировать их с помощью **#. Телефон интерпретирует такую последовательность действий как операцию **#**, которая служит для перезагрузки телефона.

Для блокировки параметров после разблокировки подождите по крайней мере 10 секунд, прежде чем снова нажать **#.

3. Перейдите к параметру DHCP Enabled и нажмите функциональную клавишу **Yes** для активизации DHCP.
4. Нажмите функциональную клавишу **Save**.

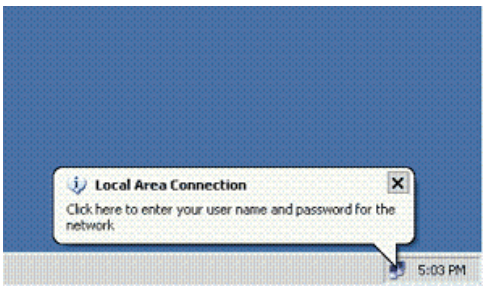
Проверка

Используйте этот раздел для проверки правильности работы конфигурации.

Клиентский ПК

Если конфигурация выполнена правильно, ПК-клиенты отобразят всплывающее предложение на ввод имени пользователя и пароля.

1. Нажмите это предложение, как показано в примере:



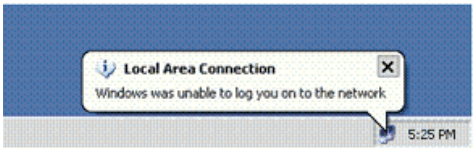
Отобразится окно для ввода имени пользователя и пароля.

Примечание. MDA не регламентирует строгий порядок аутентификации устройства. Однако для наилучших результатов компания Cisco рекомендует проводить аутентификацию голосового устройства до аутентификации устройства передачи данных на порту с активизированным MDA.

2. Введите имя пользователя и пароль.

3. Если сообщение об ошибке отсутствует, проверьте возможность подключения с помощью стандартных методов, таких как доступ к сетевым ресурсам и с помощью **ping**.

Примечание. Если отображается это сообщение об ошибке, проверьте правильность ввода имени пользователя и пароля:



IP-телефоны

С помощью меню 802.1X Authentication Status (состояние аутентификации по стандарту 802.1X) в IP-телефонах можно просматривать состояние аутентификации.

1. Нажмите кнопку **Settings**, чтобы получить доступ к параметрам "802.1X Authentication Real-Time Stats" (текущее состояние аутентификации по стандарту 802.1X), выберите **Security Configuration > 802.1X Authentication Status**.

2. Для параметра **Transaction Status** должно быть установлено значение **Authenticated**. Дополнительные сведения см. в разделе Текущее состояние аутентификации по стандарту 802.1X.

   Примечание. Проверку состояния аутентификации можно также выполнять в меню **Settings > Status > Status Messages**.

Коммутатор уровня 3

Если пароль и имя пользователя указаны верно, проверьте состояние порта 802.1x на коммутаторе.

1. Найдите значение состояния порта: AUTHORIZED (авторизован).

```
Cat-3560#show dot1x all summary
Interface       PAE     Client          Status
---------------------------------------------------------
Fa0/1           AUTH    0016.3633.339c  AUTHORIZED
                        0017.59e7.492c  AUTHORIZED
Fa0/2           AUTH    0014.5e94.5f99  AUTHORIZED
Fa0/3           AUTH    0011.858D.9AF9  AUTHORIZED
Fa0/4           AUTH    0016.6F3C.A342  AUTHORIZED
                        001a.2f80.381f  AUTHORIZED


Cat-3560#show dot1x interface fastEthernet 0/1 details

Dot1x Info for FastEthernet0/1
-----------------------------------
PAE                     = AUTHENTICATOR
PortControl             = AUTO
ControlDirection        = Both
HostMode                = MULTI_DOMAIN
ReAuthentication        = Enabled
QuietPeriod             = 10
ServerTimeout           = 30
SuppTimeout             = 30
ReAuthPeriod            = 60 (Locally configured)
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
RateLimitPeriod         = 0
Auth-Fail-Vlan          = 6
Auth-Fail-Max-attempts  = 2
Guest-Vlan              = 6

Dot1x Authenticator Client List
-------------------------------
Domain                  = DATA
Supplicant              = 0016.3633.339c
   Auth SM State        = AUTHENTICATED
   Auth BEND SM State   = IDLE
Port Status             = AUTHORIZED
ReAuthPeriod            = 60
ReAuthAction            = Reauthenticate
TimeToNextReauth        = 29
Authentication Method   = Dot1x
Authorized By           = Authentication Server
Vlan Policy             = 4

Domain                  = VOICE
Supplicant              = 0017.59e7.492c
   Auth SM State        = AUTHENTICATED
   Auth BEND SM State   = IDLE
Port Status             = AUTHORIZED
ReAuthPeriod            = 60
ReAuthAction            = Reauthenticate
TimeToNextReauth        = 15
```

```
Authentication Method     = Dot1x
Authorized By             = Authentication Server
```

Проверьте состояние VLAN после успешной аутентификации.

```
Cat-3560#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                Gi0/2
2    SERVER                           active    Fa0/24
3    VOICE                            active    Fa0/1, Fa0/4
4    MARKETING                        active    Fa0/1, Fa0/2
5    SALES                            active    Fa0/3, Fa0/4
6    GUEST_and_AUTHFAIL               active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
!--- Выходные данные команды подавлены.
```

2. Проверьте статус привязки к DHCP после успешной аутентификации.

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.3.2       0100.1759.e749.2c       Aug 24 2007 06:35 AM    Automatic
172.16.3.3       0100.1a2f.8038.1f       Aug 24 2007 06:43 AM    Automatic
172.16.4.2       0100.1636.3333.9c       Aug 24 2007 06:50 AM    Automatic
172.16.4.3       0100.145e.945f.99       Aug 24 2007 08:17 AM    Automatic
172.16.5.2       0100.166F.3CA3.42       Aug 24 2007 08:23 AM    Automatic
172.16.5.3       0100.1185.8D9A.F9       Aug 24 2007 08:51 AM    Automatic
```

Средство Интерпретатор выходных данных (только для зарегистрированных пользователей) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра анализа выходных данных команды **show**.

Поиск и устранение неполадок

Ошибки аутентификации IP-телефонов

Если не удается выполнить аутентификацию по стандарту 802.1x, статус IP-телефона отображается как `Configuring IP` (выполняется настройка IP) или `Registering` (выполняется регистрация). Чтобы устранить эту неполадку, выполните следующие действия:

- Проверьте, что 802.1x на IP-телефоне активизирован.
- Убедитесь, что идентификатор устройства введен на сервере аутентификации (RADIUS) в качестве имени пользователя.
- Убедитесь, что общий секретный ключ на IP-телефоне настроен.
- Если общий секретный ключ настроен, убедитесь, что такой же ключ введен на сервере аутентификации.
- Проверьте правильности настройки других необходимых устройств, таких как коммутатор и сервер аутентификации.

Дополнительные сведения

- **Настройка аутентификации на основе портов по стандарту IEEE 802.1x**

- **Настройка IP-телефона для использования аутентификации по стандарту 802.1x**
- **Рекомендации по развертыванию Cisco Secure ACS для серверов Windows NT/2000 в среде коммутатора Cisco Catalyst**
- **RFC 2868: атрибуты RADIUS для поддержки протокола туннеля**
- **Пример настройки аутентификации по стандарту IEEE 802.1x с использованием Catalyst 6500/6000 с ПО Cisco IOS**
- **Пример настройки аутентификации по стандарту IEEE 802.1x с использованием Catalyst 6500/6000 с ПО Cisco CatOS**
- **Страницы поддержки продуктов для LAN**
- **Страница поддержки коммутационных решений для LAN**
- **Cisco Systems – техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/100283/8021x-cat-layer3.shtml

---