Пример настройки аутентификации по стандарту IEEE 802.1x с использованием Catalyst 6500/6000 с ПО Cisco IOS

Содержание

Введение

Этот документ поясняет, как настроить IEEE 802.1x на коммутаторе Catalyst 6500/6000, работающем в собственном режиме (единый образ программного обеспечения Cisco IOS® для ядра супервизора и платы MSFC), а также службу RADIUS для аутентификации и назначения сетей VLAN.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам:

- Руководство по установке для Cisco Secure ACS для Windows 4.1
- Руководство пользователя для сервера контроля безопасного доступа (ACS) Cisco версии 4.1
- Каков принцип работы RADIUS?

- Инструкции по развертыванию коммутатора Catalyst и ACS

Используемые компоненты

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

- Catalyst 6500, который выполняет программное обеспечение Cisco IOS версии 12.1(18)SFX на Supervisor Engine**Примечание:** Для поддержки аутентификации на основе портов 802.1x требуется Cisco IOS Software Release 12.1(13)E или более поздней.
- В данном примере в качестве RADIUS-сервера используется сервер контроля безопасного доступа (ACS) Cisco версии 4.1.**Примечание:** Сервер RADIUS должен быть задан перед включением 802.1x на коммутаторе.
- Клиенты ПК, поддерживающие аутентификацию 802.1x**Примечание:** Данный пример использует клиентов Microsoft Windows XP.

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

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

Общие 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. 802.1x управляет доступом к сети путем создания двух отдельных виртуальных точек доступа в каждом порту. 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 сервисам, 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.

Примечание: Если коммутатор получает пакеты EAPOL от порта, который не настроен для аутентификации 802.1x или если коммутатор не поддерживает аутентификацию 802.1x, то пакеты EAPOL отброшены и не переданы ни к каким устройствам восходящего потока данных.

Настройка

В этом разделе вам предоставляют информацию по настройке функция 802.1x, описанная в

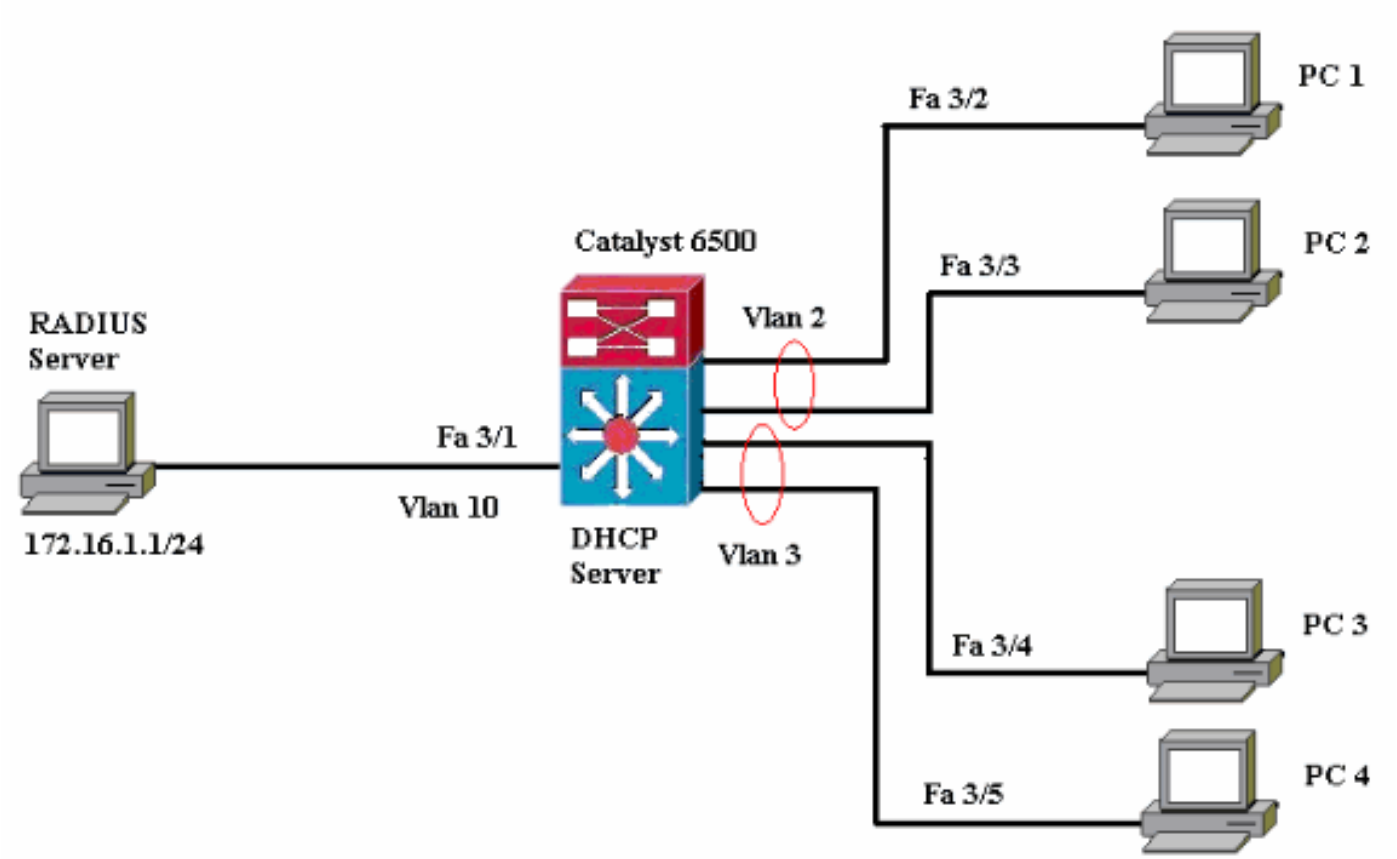
этом документе.

В данной процедуре настройки необходимо выполнить следующие шаги:

- Настройте Коммутатор Catalyst для аутентификации 802.1x.
- Настройка RADIUS-сервера.
- Настройка клиентов ПК для использования аутентификации по стандарту 802.1x.

Схема сети

В настоящем документе используется следующая схема сети:



- Сервер RADIUS — Выполняет реальную аутентификацию клиента. RADIUS-сервер проверяет подлинность клиента и передает коммутатору решение об авторизации клиента и получении им доступа к сети LAN и сервисам коммутатора. Здесь, сервер RADIUS настроен для аутентификации и назначения VLAN.
- Коммутатор — Управляет физическим доступом к сетевому на статусе проверки подлинности 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. Здесь, Коммутатор Catalyst 6500 также настроен как сервер DHCP. Поддержка функции аутентификации 802.1x для Протокола DHCP (динамического конфигурирования узла) позволяет серверу DHCP назначать IP-адреса на другие классы конечных пользователей путем добавления идентификатора аутентифицированного пользователя в процесс обнаружения DHCP.
- Клиенты — устройства (рабочие станции), который запрашивает доступ к сервисам LAN (локальной сети) и службам коммутатора и отвечает на запросы от коммутатора. Здесь,

PC 1 - 4 являются клиентами, которые запрашивают аутентифицируемый доступ к сети. PC 1 и 2 используют те же учетные данные начала сеанса, которые находятся в VLAN 2. Точно так же PC 3 и 4 используют учетные данные начала сеанса для VLAN 3. ПК - клиенты настроены для достижения IP-адреса от сервера DHCP.

Настройте коммутатор Catalyst для аутентификации 802.1x

В пример настройки коммутатора входит:

- Как включить аутентификацию 802.1x на Портах FastEthernet.
- Как подключить сервер RADIUS с VLAN 10 позади Порта FastEthernet 3/1.
- Конфигурация сервера DHCP для двух пулов IP, один для клиентов в VLAN 2 и другом для клиентов в VLAN 3.
- Маршрутизация между сетями VLAN для установки подключения между клиентами после выполнения аутентификации.

См. 802.1x Рекомендации по Аутентификации На основе порта и Ограничения для рекомендаций по тому, как настроить аутентификацию 802.1x.

Примечание: Удостоверьтесь, что сервер RADIUS всегда соединяется позади авторизованного порта.

Catalyst 6500

```
Router#configure terminal Enter configuration commands,
one per line. End with CNTL/Z. Router(config)#hostname
Cat6K !--- Sets the hostname for the switch.
Cat6K(config)#vlan 2 Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3 Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER !--- This is a
dedicated VLAN for the RADIUS server. Cat6K(config-
vlan)#exit Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport Cat6K(config-if)#switchport
mode access Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut !--- Assigns the port connected
to the RADIUS server to VLAN 10. !--- Note:- All the
active access ports are in VLAN 1 by default.
Cat6K(config-if)#exit Cat6K(config)#dot1x system-auth-
control !--- Globally enables 802.1x.
Cat6K(config)#interface range fastEthernet3/2-48
Cat6K(config-if-range)#switchport Cat6K(config-if-
range)#switchport mode access Cat6K(config-if-
range)#dot1x port-control auto Cat6K(config-if-range)#no
shut !--- Enables 802.1x on all the FastEthernet
interfaces. Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model !--- Enables AAA.
Cat6K(config)#aaa authentication dot1x default group
radius !--- Method list should be default. Otherwise
dot1x does not work. Cat6K(config)#aaa authorization
network default group radius !--- You need authorization
for dynamic VLAN assignment to work with RADIUS.
Cat6K(config)#radius-server host 172.16.1.1 !--- Sets
the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco !--- The key must
match the key used on the RADIUS server.
Cat6K(config)#interface vlan 10 Cat6K(config-if)#ip
address 172.16.1.2 255.255.255.0 Cat6K(config-if)#no
```

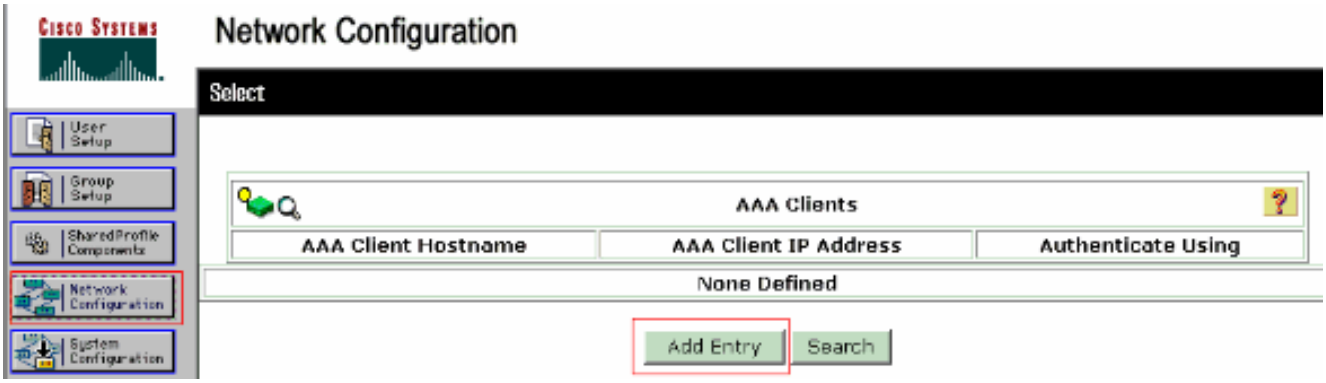
```
shut !--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut !--- This is the gateway
address for clients in VLAN 2. Cat6K(config-
if)#interface vlan 3 Cat6K(config-if)#ip address
172.16.3.1 255.255.255.0 Cat6K(config-if)#no shut !---
This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit Cat6K(config)#ip dhcp pool
vlan2_clients Cat6K(dhcp-config)#network 172.16.2.0
255.255.255.0 Cat6K(dhcp-config)#default-router
172.16.2.1 !--- This pool assigns ip address for clients
in VLAN 2. Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1 !--- This
pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit Cat6K(config)#ip dhcp excluded-
address 172.16.2.1 Cat6K(config)#ip dhcp excluded-
address 172.16.3.1 Cat6K(config-if)#end Cat6K#show vlan
VLAN Name Status Ports ---- ------------------------------
---- --------- ------------------------------ 1 default
active Fa3/2, Fa3/3, Fa3/4, Fa3/5 Fa3/6, Fa3/7, Fa3/8,
Fa3/9 Fa3/10, Fa3/11, Fa3/12, Fa3/13 Fa3/14, Fa3/15,
Fa3/16, Fa3/17 Fa3/18, Fa3/19, Fa3/20, Fa3/21 Fa3/22,
Fa3/23, Fa3/24, Fa3/25 Fa3/26, Fa3/27, Fa3/28, Fa3/29
Fa3/30, Fa3/31, Fa3/32, Fa3/33 Fa3/34, Fa3/35, Fa3/36,
Fa3/37 Fa3/38, Fa3/39, Fa3/40, Fa3/41 Fa3/42, Fa3/43,
Fa3/44, Fa3/45 Fa3/46, Fa3/47, Fa3/48 2 VLAN2 active 3
VLAN3 active 10 RADIUS_SERVER active Fa3/1 1002 fddi-
default act/unsup 1003 token-ring-default act/unsup 1004
fddinet-default act/unsup 1005 trnet-default act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Настройка RADIUS-сервера

Сервер RADIUS настроен со статическим IP - адресом 172.16.1.1/24. Выполните эти шаги для настройки сервера RADIUS для клиента AAA:

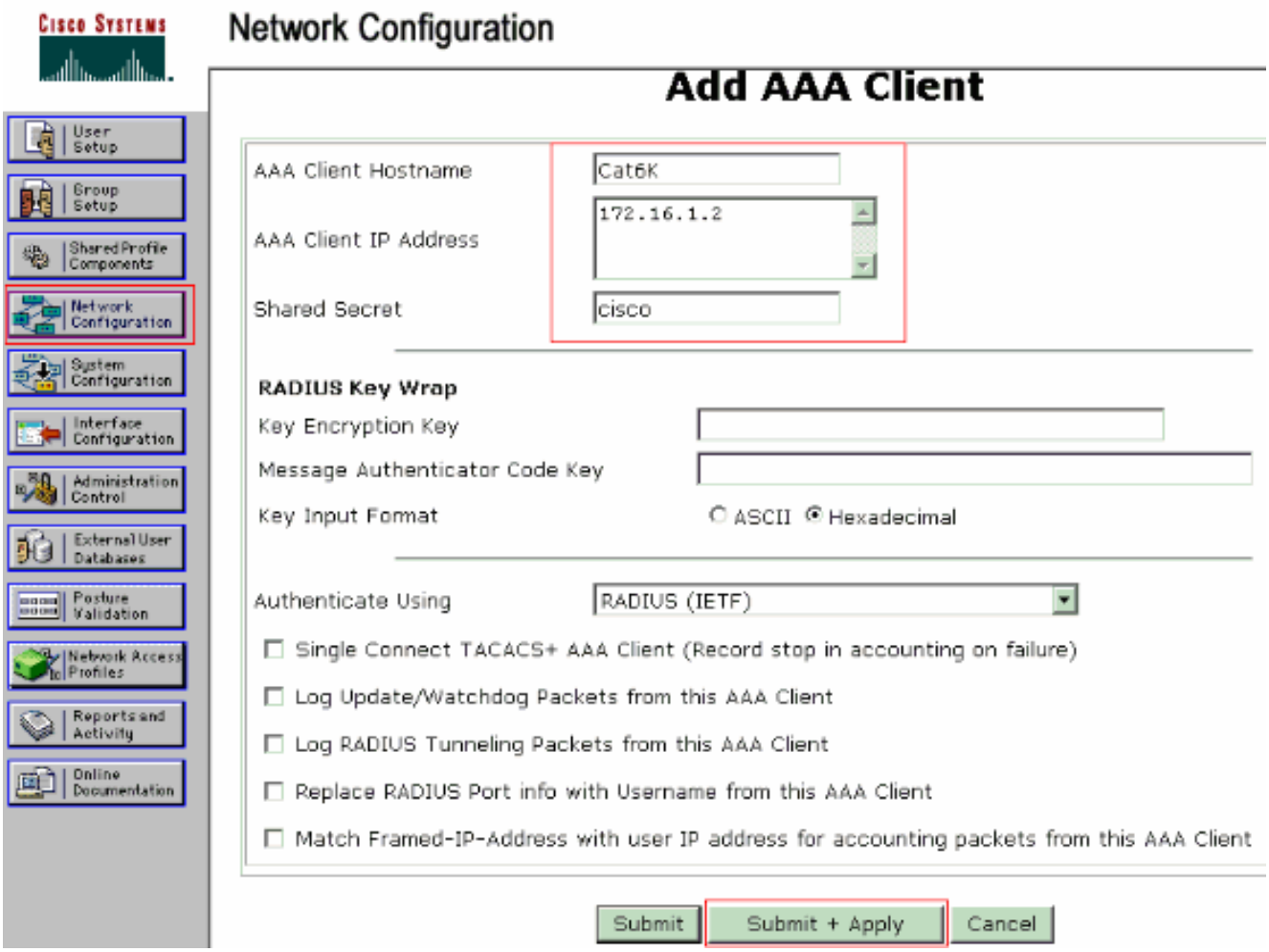
1. Нажмите Network Configuration в окне управления ACS для настройки AAA-клиента.
2. Нажмите Add Entry в разделе клиентов AAA.



3. Определите для AAA-клиента имя хоста, IP-адрес, общий секретный ключ и тип

аутентификации следующим образом:Имя хоста для клиента AAA = имя хоста коммутатора **(Cat6K)**.IP-адрес клиента AAA = IP-адрес Интерфейса управления **коммутатора (172.16.1.2)**.Общий секретный ключ = настроенный ключ RADIUS на коммутаторе **(Cisco)**.Используемая аутентификация = **IETF RADIUS**.**Примечание:** Для нормальной работы общий секретный ключ должен быть идентичным на клиенте AAA и ACS. При использовании ключей необходимо учитывать регистр.

4. Нажмите **Submit + Применяются** для внесения этих изменений эффективными, как показано в
примере:

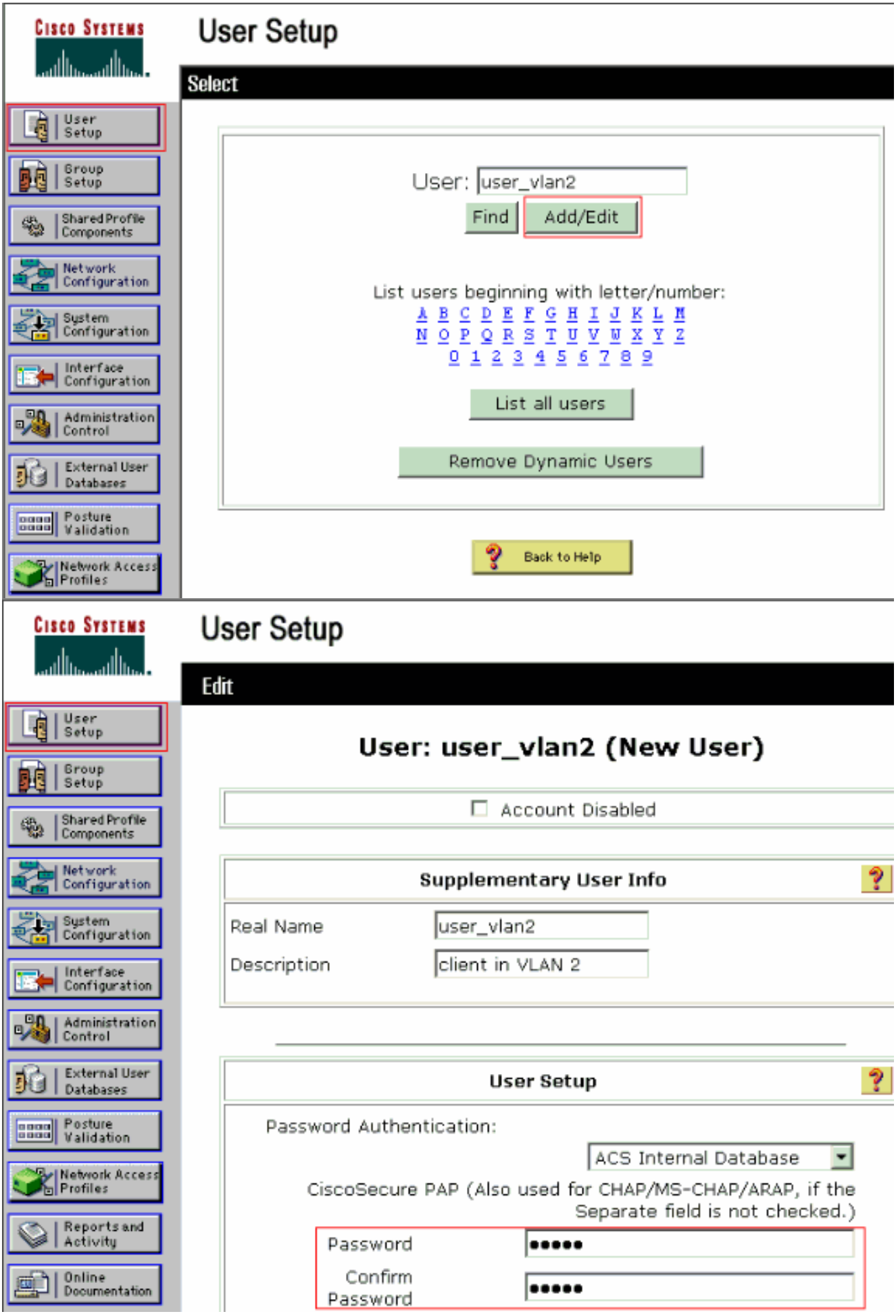


Выполните эти шаги для настройки сервера RADIUS для аутентификации, VLAN и присвоения IP-адреса.

Два имен пользователей должны быть созданы отдельно для клиентов, которые соединяются с VLAN 2, а также для VLAN 3. Здесь, пользователь **user_vlan2** для клиентов, которые соединяются с VLAN 2 и другим пользователем **user_vlan3** для клиентов, которые соединяются с VLAN 3, создан для этой цели.

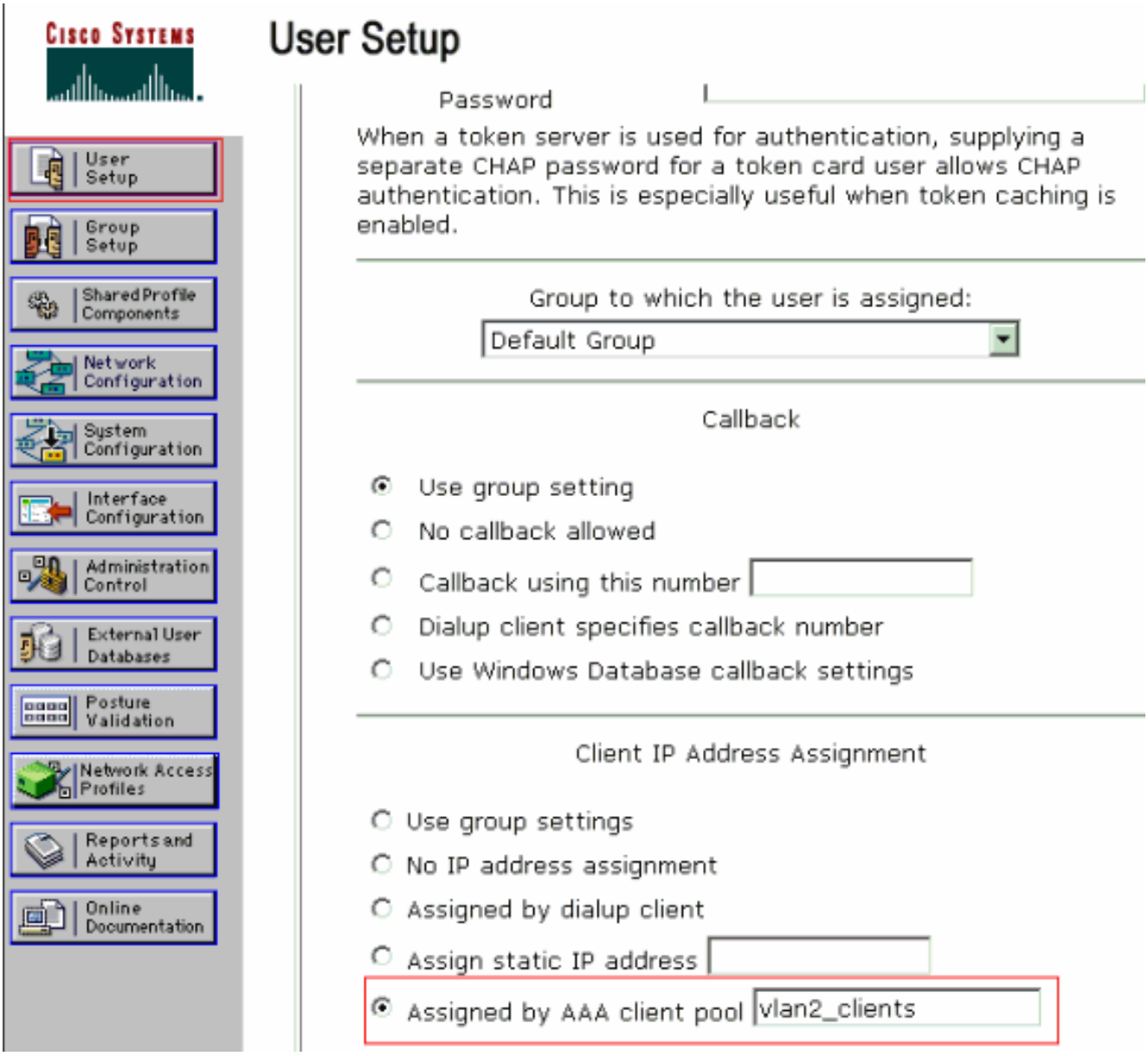
Примечание: Здесь, пользовательскую конфигурацию показывают для клиентов, которые соединяются с VLAN 2 только. Для пользователей, которые соединяются с VLAN 3, выполните ту же процедуру.

1. Чтобы добавить и настроить пользователей, нажмите **User Setup** и определите имя пользователя и
пароль.



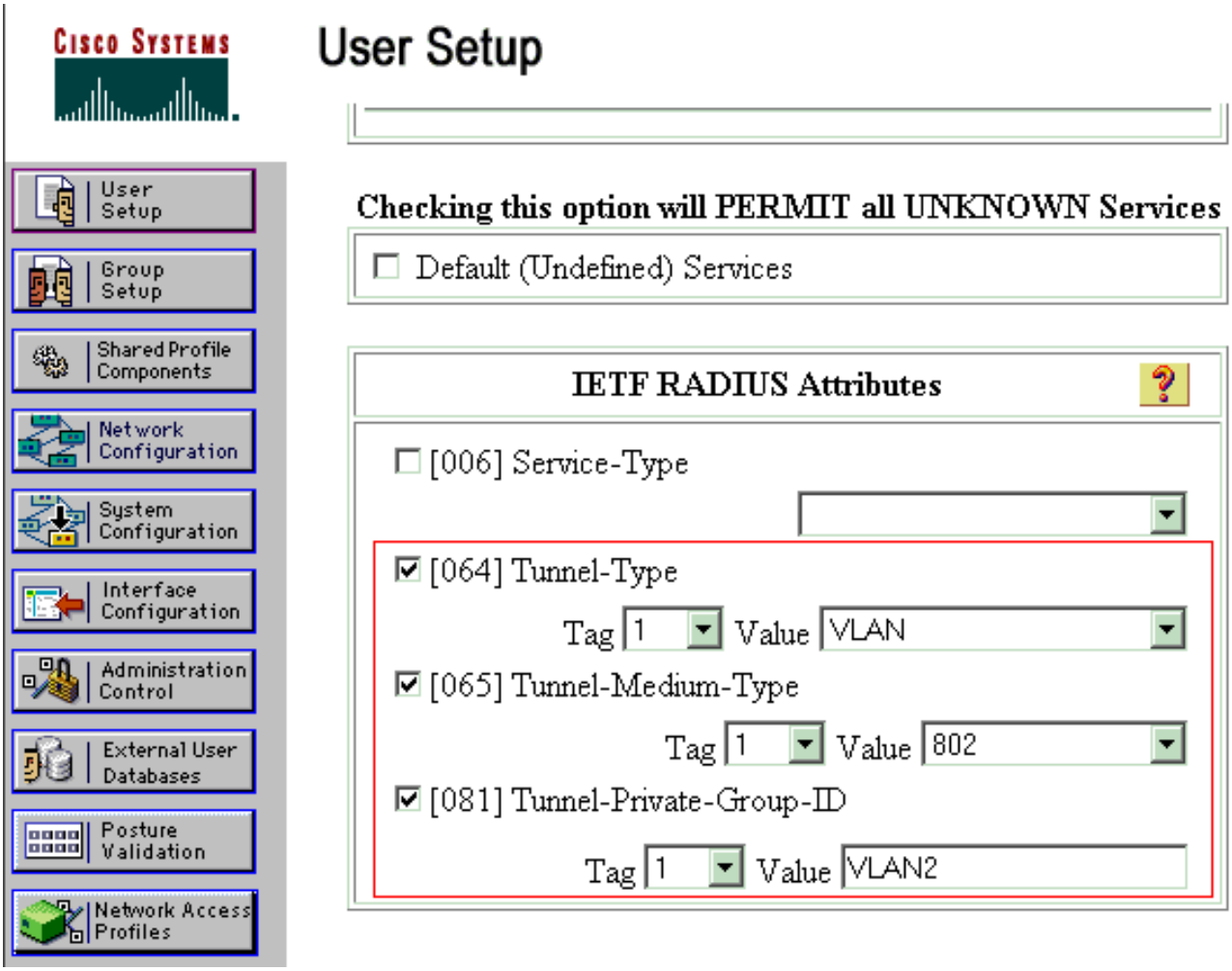
2. **Определите назначение IP-адреса клиента как Assigned by AAA client pool (назначенный из пула клиентов AAA-сервера).** Введите имя назначенного из пула IP-

адресов на коммутаторе для клиентов VLAN 2.



Примечание: Выберите эту опцию и введите имя пула IP клиента AAA в коробке, только если этому пользователю нужно было назначить IP-адрес назначенным из пула IP-адресов на клиенте AAA.

3. Определите атрибуты инженерной группы по развитию Интернета (IETF) **64** и **65.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:** При использовании *названия* VLAN это должно быть точно то же как то, настроенное в коммутаторе.



Примечание: Для получения дополнительной информации об этих атрибутах IETF обратитесь к RFC 2868: Атрибуты RADIUS для поддержки туннельного протокола.**Примечание:** В начальной конфигурации сервера ACS атрибуты RADIUS IETF могут быть не в состоянии отображаться в **Настройке пользователя**. **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 вы не определяете атрибут IETF **81**, и порт является портом коммутатора в режиме доступа, у клиента есть присвоение на VLAN доступа порта. Если вы определили атрибут **81** для динамического назначения сетей VLAN, и порт является портом коммутатора в режиме доступа, необходимо выполнить **команду aaa authorization network default group radius** на коммутаторе. Данная команда назначает порт сети VLAN, которую обеспечивает сервер RADIUS. `802.1x AUTHORIZED () . - VLAN` . Если вы определили атрибут **81**, но вы настроили порт как маршрутизируемый порт, отказ в доступе происходит. Это сообщение об ошибках показывает:`%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE: RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose VLAN cannot be assigned.`

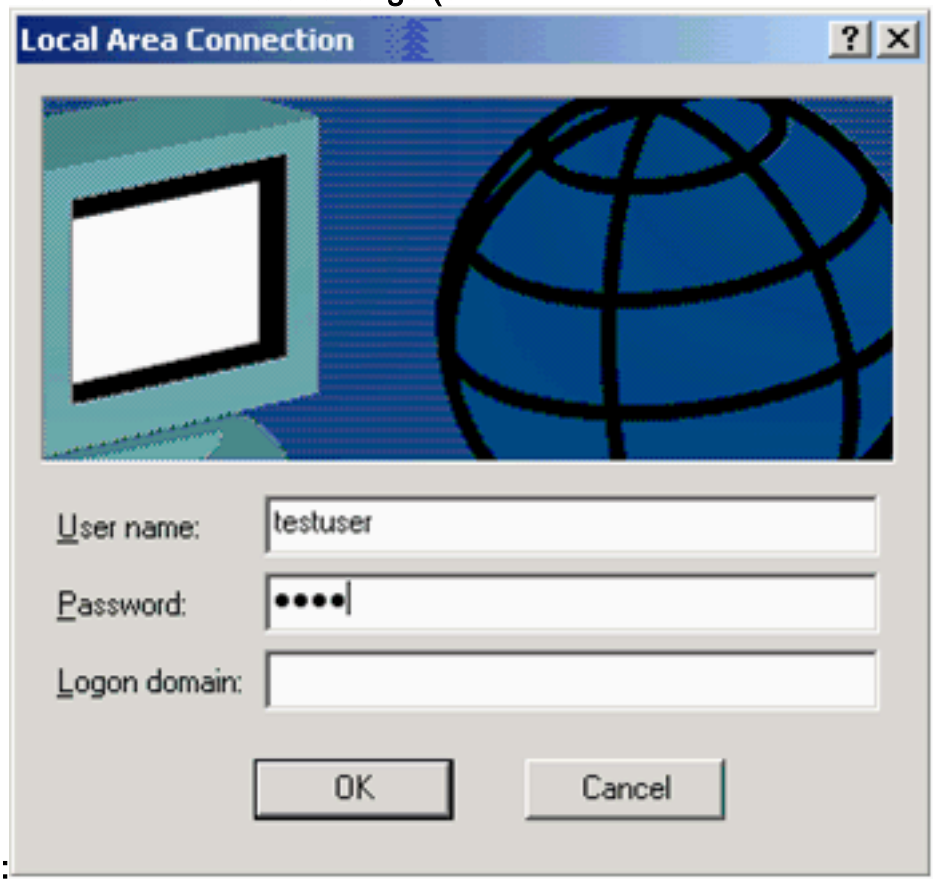
Настройка клиентов ПК для использования аутентификации по стандарту 802.1x

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.

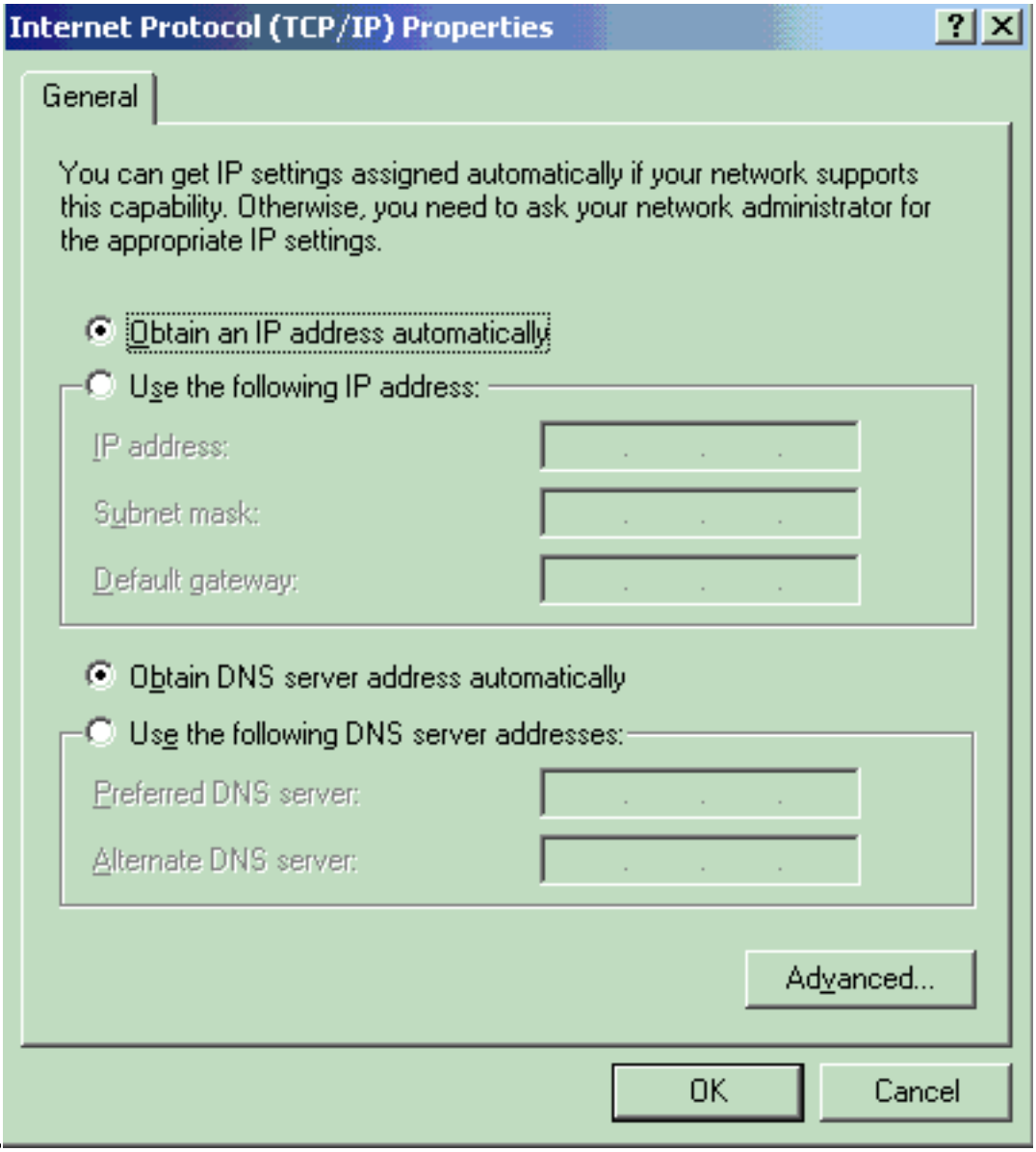


пример):

Выполните эти шаги для настройки клиентов для получения IP-адреса из сервера DHCP.

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

автоматически).

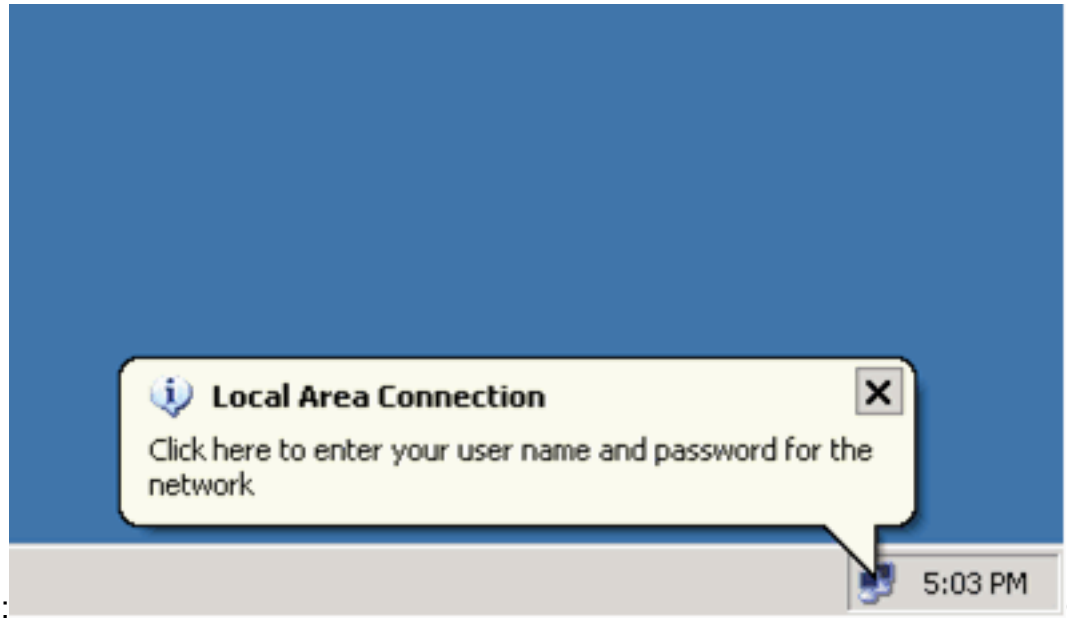


Проверка

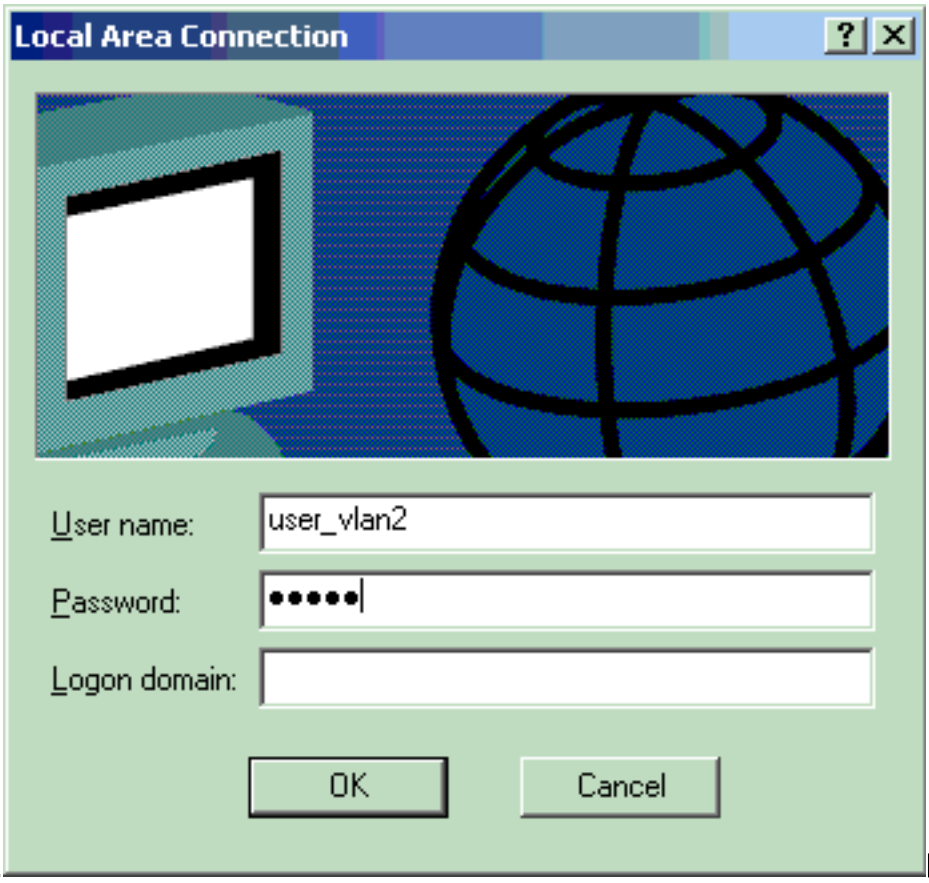
Клиентский ПК

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

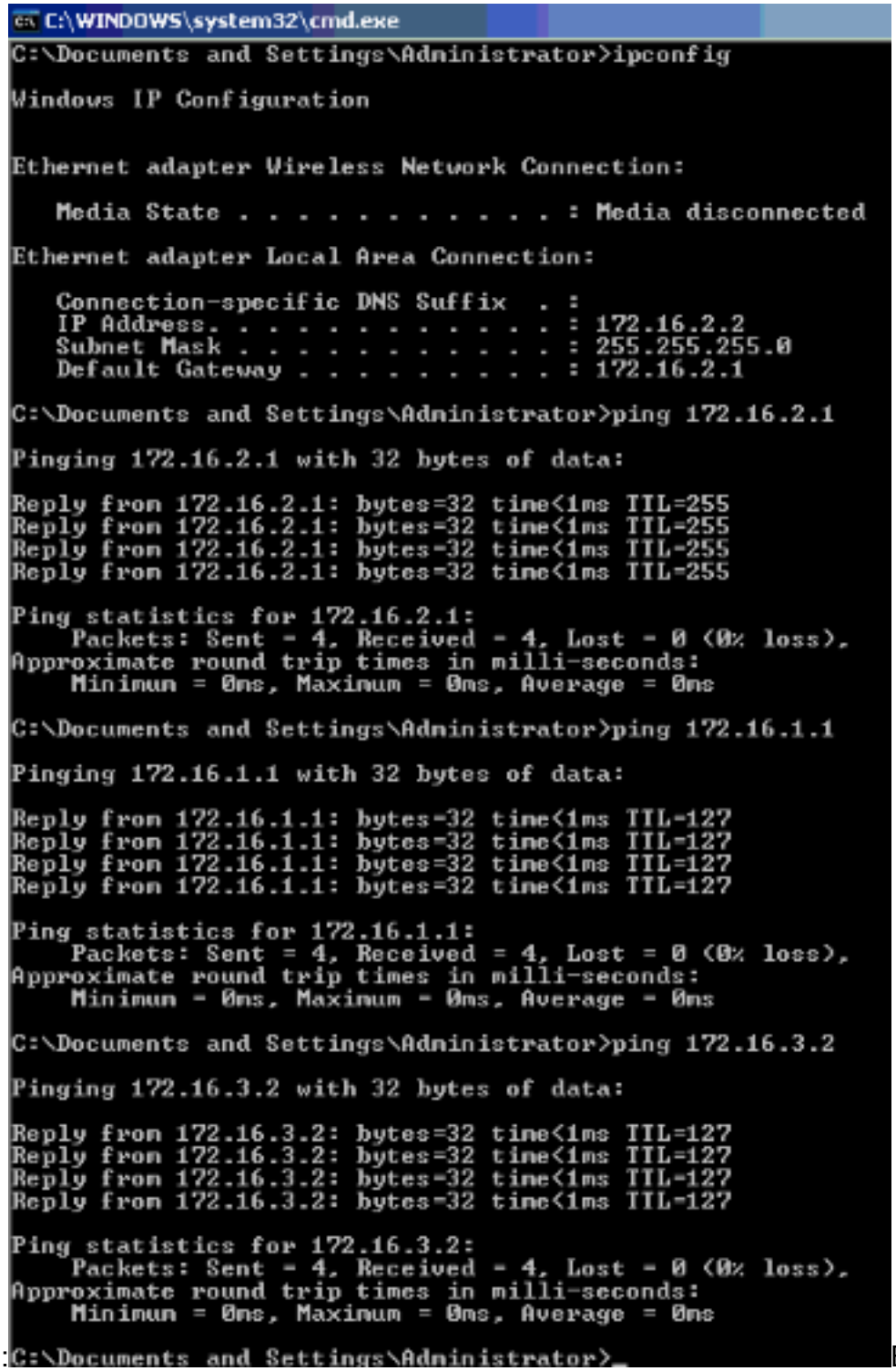
1. Нажмите это предложение, как показано в

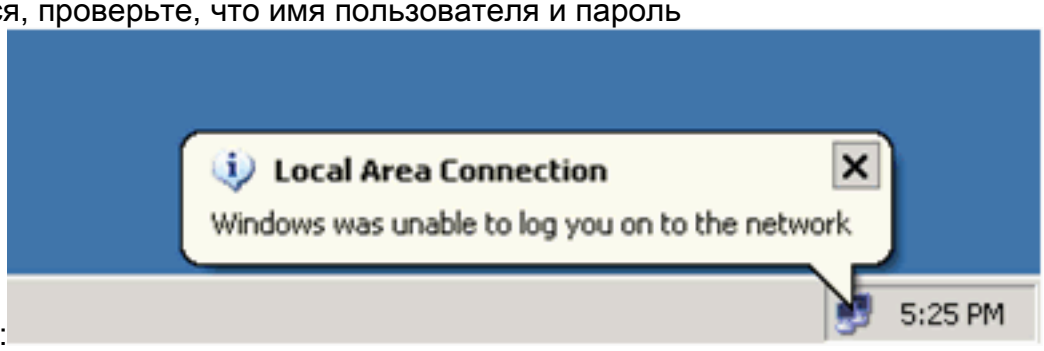
примере: 

Отобразится окно для ввода имени пользователя и пароля.

2. Введите имя пользователя и пароль. 

Примечание: В ПК 1 и 2, введите учетные данные пользователя VLAN 2 и в ПК 3, и 4 вводят VLAN 3 учетных данных пользователя.
3. **Если сообщение об ошибке отсутствует, проверьте возможность подключения с помощью стандартных методов, таких как доступ к сетевым ресурсам и с помощью ping.** Эти выходные данные от ПК 1 и показывают **успешное завершение команды ping**



ПК 4:Если эта ошибка появляется, проверьте, что имя пользователя и пароль корректно: 

Catalyst 6500

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

коммутаторе.

1. : AUTHORIZED ().Cat6K#**show dot1x** Sysauthcontrol = **Enabled** Dot1x Protocol Version = 1 Dot1x Oper Controlled Directions = Both Dot1x Admin Controlled Directions = Both Cat6K#**show dot1x interface fastEthernet 3/2** AuthSM State = AUTHENTICATED BendSM State = IDLE **PortStatus = AUTHORIZED** MaxReq = 2 MultiHosts = Enabled Port Control = Auto QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Cat6K#**show dot1x interface fastEthernet 3/4** AuthSM State = AUTHENTICATED BendSM State = IDLE **PortStatus = AUTHORIZED** MaxReq = 2 MultiHosts = Enabled Port Control = Auto QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Cat6K#**show dot1x interface fastEthernet 3/1** Default Dot1x Configuration Exists for this interface FastEthernet3/1 AuthSM State = FORCE AUTHORIZED BendSM State = IDLE **PortStatus = AUTHORIZED** MaxReq = 2 MultiHosts = Disabled PortControl = Force Authorized QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Проверьте состояние VLAN после успешной аутентификации.Cat6K#**show vlan** VLAN Name Status Ports ---- ------------------------------ --------- ------------------- ----------- 1 default active Fa3/6, Fa3/7, Fa3/8, Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13, Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19, Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25, Fa3/26, Fa3/27, Fa3/28, Fa3/29, Fa3/30, Fa3/31, Fa3/32, Fa3/33, Fa3/34, Fa3/35, Fa3/36, Fa3/37, Fa3/38, Fa3/39, Fa3/40, Fa3/41, Fa3/42, Fa3/43, Fa3/44, Fa3/45, Fa3/46, Fa3/47, Fa3/48 **2 VLAN2 active Fa3/2, Fa3/3 3 VLAN3 active Fa3/4, Fa3/5** 10 RADIUS_SERVER active Fa3/1 1002 fddi-default act/unsup 1003 token-ring-default act/unsup 1004 fddinet-default act/unsup 1005 trnet-default act/unsup *!--- Output suppressed.*
2. Проверьте статус привязки к DHCP от после успешной аутентификации.Router#**show ip dhcp binding** IP address Hardware address Lease expiration Type 172.16.2.2 0100.1636.3333.9c Mar 04 2007 06:35 AM Automatic 172.16.2.3 0100.166F.3CA3.42 Mar 04 2007 06:43 AM Automatic 172.16.3.2 0100.145e.945f.99 Mar 04 2007 06:50 AM Automatic 172.16.3.3 0100.1185.8D9A.F9 Mar 04 2007 06:57 AM Automatic Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Устранение неполадок

Соберите выходные данные этих **команд отладки** для устранения проблем:

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

- **события debug dot1x** — Включают отладку операторов печати, которые охраняет флаг событий dot1x.Cat6K#**debug dot1x events** Dot1x events debugging is on Cat6K# *!--- Debug output for PC 1 connected to Fa3/2.* 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0 00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 **00:13:36: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/2** 00:13:36: dot1x-ev:MAC Address is 0016.3633.339c 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36: dot1x-ev:going to send to backend on SP, length = 6 00:13:36: dot1x-ev:Sent to Bend 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15 00:13:36: dot1x-ev:Found a process thats already handling therequest for this id 12 00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36: dot1x-ev:going to send to backend on SP, length = 31 00:13:36: dot1x-ev:Sent to Bend 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16 00:13:36: dot1x-ev:Found a process thats already handling therequest for this id 13 **00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32 00:13:36:**

dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:13:36: dot1x-ev:Vlan name = VLAN2 00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 16 EAP pkt len = 4 00:13:37: dot1x-ev:The process finished processing the request will pick up any pending requests from the queue Cat6K# Cat6K# *!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0 00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/4** 00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:19:58: dot1x-ev:going to send to backend on SP, length = 6 00:19:58: dot1x-ev:Sent to Bend 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9 00:19:58: dot1x-ev:Found a process thats already handling therequest for this id 10 00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:19:58: dot1x-ev:going to send to backend on SP, length = 31 00:19:58: dot1x-ev:Sent to Bend 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10 00:19:58: dot1x-ev:Found a process thats already handling therequest for this id 11 **00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:19:58: dot1x-ev:Vlan name = 3** 00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4 00:19:58: dot1x-ev:The process finished processing the request will pick up any pending requests from the queue Cat6K#

- **debug radius – отображает связанную с RADIUS информацию.**Cat6K#**debug radius** Radius protocol debugging is on Cat6K# *!--- Debug output for PC 1 connected to Fa3/2.* 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18 CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79 00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80 18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104 00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19 172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80 18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124 00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8 01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36: Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18 11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# *!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11 172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login: length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:

```
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 109 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12
172.16.1.1:1812, Access-Request, len 109 00:19:58: Attribute 4 6 AC100201 00:19:58:
Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8
00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80
18 F4C8832E 00:19:58: RADIUS: Received from id 12 172.16.1.1:1812, Access-Challenge, len 104
00:19:58: Attribute 79 33 010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80
18 45472A93 00:19:58: RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-
login: got challenge from radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 135 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13
172.16.1.1:1812, Access-Request, len 135 00:19:58: Attribute 4 6 AC100201 00:19:58:
Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8
00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80
18 37011E8F 00:19:58: RADIUS: Received from id 13 172.16.1.1:1812, Access-Accept, len 120
00:19:58: Attribute 64 6 0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4
0133580F 00:19:58: Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58:
Attribute 79 6 030C0004 00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18
F5520A95 00:19:58: RADIUS: EAP-login: length of eap packet = 4 Cat6K#
```

Дополнительные сведения

- Пример настройки аутентификации по стандарту IEEE 802.1x с использованием Catalyst 6500/6000 с ПО Cisco CatOS
- Рекомендации по развертыванию Cisco Secure ACS для серверов Windows NT/2000 в среде коммутатора Cisco Catalyst
- Спецификация RFC 2868: Атрибуты RADIUS для поддержки туннельного протокола
- Настройка аутентификации на основе портов по стандарту IEEE 802.1x
- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация