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

Содержание

Введение

Этот документ объясняет, как настроить IEEE 802.1x на Catalyst 6500/6000, который выполняется в гибридном режиме (CatOS на Supervisor Engine и программное обеспечение Cisco IOS на MSFC) и сервер для аутентификации Сервиса RADIUS и назначение 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 Релиз прогрммного обеспечения Catos 8.5 (6) на Supervisor Engine и программном обеспечении Cisco IOS версии 12.1(18)SFX на MSFC**Примечание:** Вам нужен Выпуск 6.2 CatOS или позже поддержать 802.1x аутентификация на основе порта.**Примечание:** Перед выпуском ПО 7.2 (2), как только хост 802.1x аутентифицируется, он присоединяется к настроенной VLAN NVRAM. С версиями 7.2 (2) и позднее выпуска ПО, после аутентификации, хост 802.1x может получить свое назначение VLAN от сервера RADIUS.
- В данном примере в качестве RADIUS-сервера используется сервер контроля безопасного доступа (ACS) Cisco версии 4.1.**Примечание:** Сервер RADIUS должен быть задан прежде, чем включить 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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов 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, которое связано с портом коммутатора и назначает порт для сети VLAN прежде, чем сделать доступным любые услуги, которые предложены коммутатором или LAN. Пока устройство не аутентифицируется, управление доступом 802.1x позволяет только Протокол EAP по LAN (EAPOL) трафик через порт, с которым связано устройство. После успешного завершения аутентификации "нормальный" трафик может проходить через порт.

Настройка

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

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

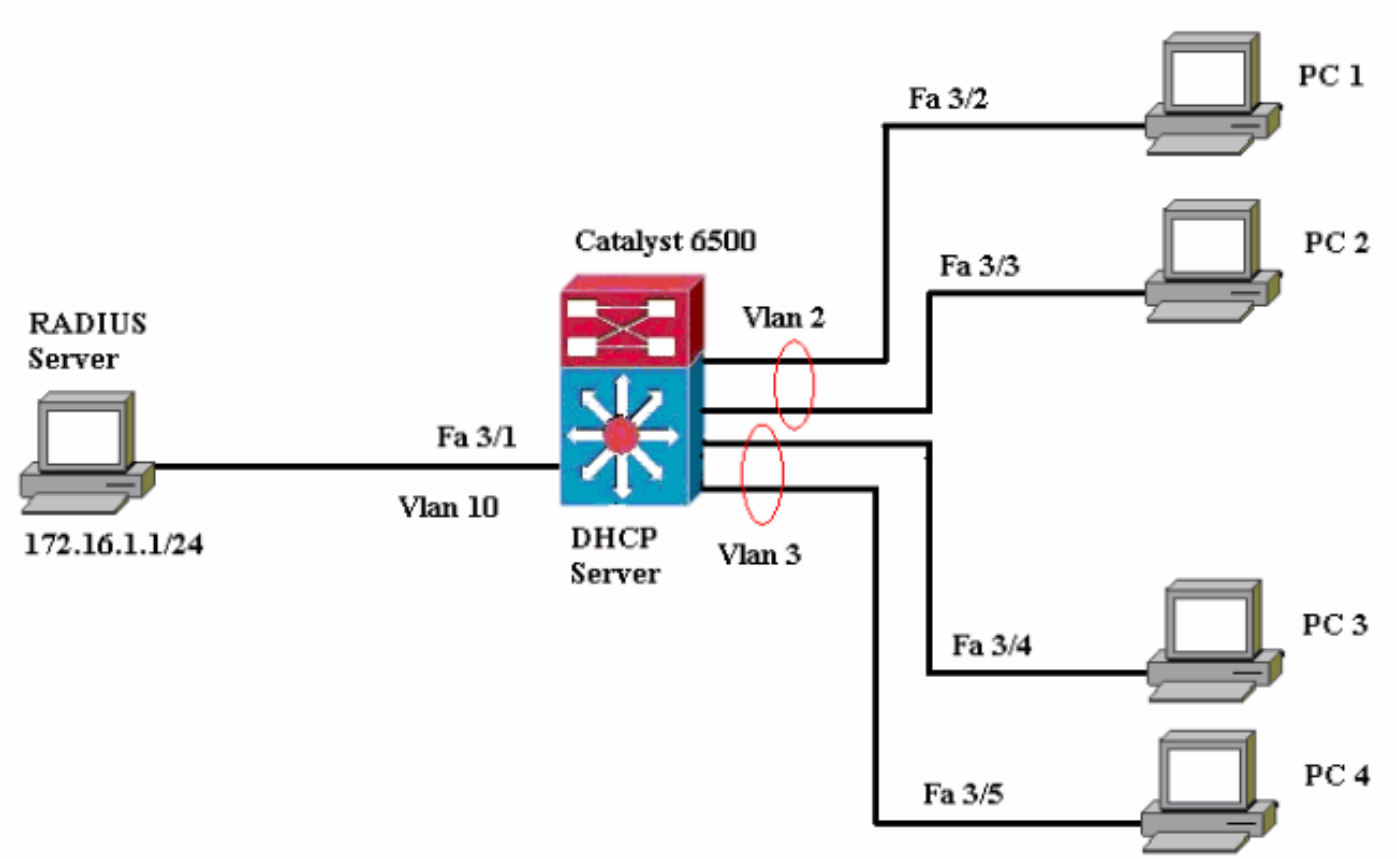
использованных в этом разделе.

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 (проксируют) между клиентом и сервером RADIUS, запрашивая идентификационную информацию от клиента, проверяя что информация с сервером RADIUS и передача ответа 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), которые запрашивают доступ к сервисам LAN (локальной сети) и службам коммутатора и отвечают на запросы от коммутатора. Здесь,

PC 1 - 4 являются клиентами, которые запрашивают аутентифицируемый доступ к сети. PC 1 и 2 будут использовать те же учетные данные начала сеанса, чтобы быть в VLAN 2. Точно так же PC 3 и 4 будут использовать учетные данные начала сеанса для VLAN 3. ПК - клиенты настроены для достижения IP-адреса от сервера DHCP.**Примечание:** В этой конфигурации любой клиент, который отказывает аутентификацию или любой не802.1x способный клиент, соединяющийся с коммутатором, является запрещенным доступом к сети путем перемещения их в неиспользованную VLAN (VLAN 4 или 5) использование функции гостевого VLAN и ошибка проверки подлинности.

Настройте коммутатор Catalyst для аутентификации 802.1x

В пример настройки коммутатора входит:

- Включите аутентификацию 802.1x и привязанные функции на Портах FastEthernet.
- Сервер RADIUS подключения к 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. Конфигурацию аутентификации Рекомендации для рекомендаций по тому, как настроить аутентификацию 802.1x.

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

Catalyst 6500

```
Console (enable) set system name Cat6K System name set.
!--- Sets the hostname for the switch. Cat6K> (enable)
set localuser user admin password cisco Added local user
admin. Cat6K> (enable) set localuser authentication
enable LocalUser authentication enabled !--- Uses local
user authentication to access the switch. Cat6K>
(enable) set vtp domain cisco VTP domain cisco modified
!--- Domain name must be configured for VLAN
configuration. Cat6K> (enable) set vlan 2 name VLAN2 VTP
advertisements transmitting temporarily stopped, and
will resume after the command finishes. Vlan 2
configuration successful !--- VLAN should be existing in
the switch !--- for a successsful authentication. Cat6K>
(enable) set vlan 3 name VLAN3 VTP advertisements
transmitting temporarily stopped, and will resume after
the command finishes. Vlan 3 configuration successful !-
-- VLAN names will be used in RADIUS server for VLAN
assignment. Cat6K> (enable) set vlan 4 name
AUTHFAIL_VLAN VTP advertisements transmitting
temporarily stopped, and will resume after the command
finishes. Vlan 4 configuration successful !--- A VLAN
for non-802.1x capable hosts. Cat6K> (enable) set vlan 5
name GUEST_VLAN VTP advertisements transmitting
temporarily stopped, and will resume after the command
finishes. Vlan 4 configuration successful !--- A VLAN
for failed authentication hosts. Cat6K> (enable) set
vlan 10 name RADIUS_SERVER VTP advertisements
transmitting temporarily stopped, and will resume after
the command finishes. Vlan 10 configuration successful
```

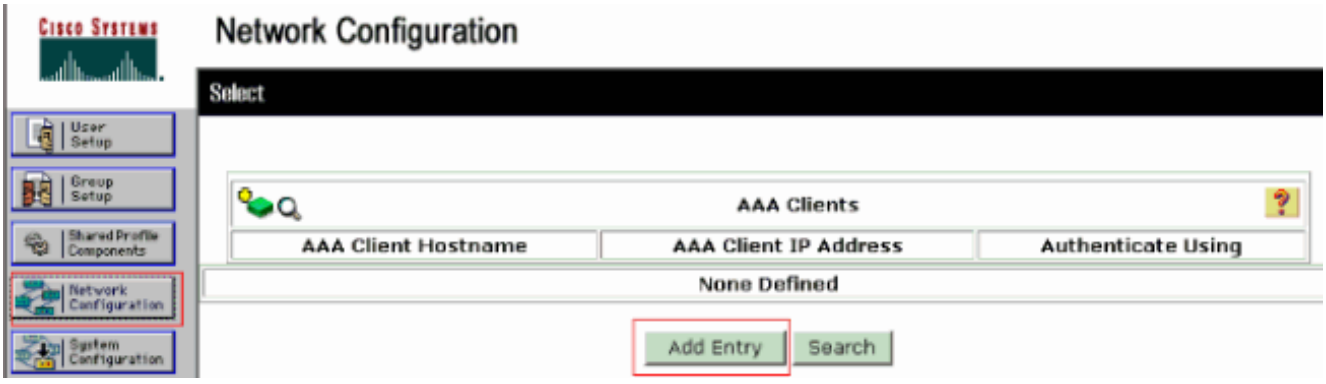
!--- This is a dedicated VLAN for the RADIUS Server.
Cat6K> (enable) **set interface sc0 10 172.16.1.2 255.255.255.0** Interface sc0 vlan set, IP address and netmask set. *!--- **Note:** 802.1x authentication always uses the !--- sc0 interface as the identifier for the authenticator !--- when communicating with the RADIUS server.* Cat6K> (enable) **set vlan 10 3/1** VLAN 10 modified. VLAN 1 modified. VLAN Mod/Ports ---- ---------- 10 3/1 *!--- Assigns port connecting to RADIUS server to VLAN 10.* Cat6K> (enable) **set radius server 172.16.1.1 primary** 172.16.1.1 with auth-port 1812 acct-port 1813 added to radius server table as primary server. *!--- Sets the IP address of the RADIUS server.* Cat6K> (enable) **set radius key cisco** Radius key set to cisco *!--- The key must match the key used on the RADIUS server.* Cat6K> (enable) **set dot1x system-auth-control enable** dot1x system-auth-control enabled. Configured RADIUS servers will be used for dot1x authentication. *!--- Globally enables 802.1x. !--- You must specify at least one RADIUS server before !--- you can enable 802.1x authentication on the switch.* Cat6K> (enable) **set port dot1x 3/2-48 port-control auto** Port 3/2-48 dot1x port-control is set to auto. Trunking disabled for port 3/2-48 due to Dot1x feature. Spantree port fast start option enabled for port 3/2-48. *!--- Enables 802.1x on all FastEthernet ports. !--- This disables trunking and enables portfast automatically.* Cat6K> (enable) **set port dot1x 3/2-48 auth-fail-vlan 4** Port 3/2-48 Auth Fail Vlan is set to 4 *!--- Ports will be put in VLAN 4 after three !--- failed authentication attempts.* Cat6K> (enable) **set port dot1x 3/2-48 guest-vlan 5** Ports 3/2-48 Guest Vlan is set to 5 *!--- Any non-802.1x capable host connecting or 802.1x !--- capable host failing to respond to the username and password !--- authentication requests from the Authenticator is placed in the !--- guest VLAN after 60 seconds. !--- **Note:** An authentication failure VLAN is independent !--- of the guest VLAN. However, the guest VLAN can be the same !--- VLAN as the authentication failure VLAN. If you do not want to !--- differentiate between the non-802.1x capable hosts and the !--- authentication failed hosts, you can configure both hosts to !--- the same VLAN (either a guest VLAN or an authentication failure VLAN). !--- For more information, refer to !--- Understanding How 802.1x Authentication for the Guest VLAN Works.* Cat6K> (enable) **switch console** Trying Router-16... Connected to Router-16. Type ^C^C^C to switch back... *!--- Transfers control to the routing module (MSFC).* Router>**enable** Router#**conf t** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#**interface vlan 10** Router(config-if)#**ip address 172.16.1.3 255.255.255.0** *!--- This is used as the gateway address in RADIUS server.* Router(config-if)#**no shut** Router(config-if)#**interface vlan 2** Router(config-if)#**ip address 172.16.2.1 255.255.255.0** Router(config-if)#**no shut** *!--- This is the gateway address for clients in VLAN 2.* Router(config-if)#**interface vlan 3** Router(config-if)#**ip address 172.16.3.1 255.255.255.0** Router(config-if)#**no shut** *!--- This is the gateway address for clients in VLAN 3.* Router(config-if)#**exit** Router(config)#**ip dhcp pool vlan2_clients** Router(dhcp-config)#**network 172.16.2.0 255.255.255.0** Router(dhcp-config)#**default-router 172.16.2.1** *!--- This pool assigns ip address for clients in VLAN 2.* Router(dhcp-config)#**ip dhcp pool**

```
vlan3_clients Router(dhcp-config)#network 172.16.3.0
255.255.255.0 Router(dhcp-config)#default-router
172.16.3.1 !--- This pool assigns ip address for clients
in VLAN 3. Router(dhcp-config)#exit Router(config)#ip
dhcp excluded-address 172.16.2.1 Router(config)#ip dhcp
excluded-address 172.16.3.1 !--- In order to go back to
the Switching module, !--- enter Ctrl-C three times.
Router# Router#^C Cat6K> (enable) Cat6K> (enable) show
vlan VLAN Name Status IfIndex Mod/Ports, Vlans ---- ----
-------------- --------- ------- ----------------------
- 1 default active 6 2/1-2 3/2-48 2 VLAN2 active 83 3
VLAN3 active 84 4 AUTHFAIL_VLAN active 85 5 GUEST_VLAN
active 86 10 RADIUS_SERVER active 87 3/1 1002 fddi-
default active 78 1003 token-ring-default active 81 1004
fddinet-default active 79 1005 trnet-default active 80
!--- Output suppressed. !--- All active ports will be in
VLAN 1 (except 3/1) before authentication. Cat6K>
(enable) show dot1x PAE Capability Authenticator Only
Protocol Version 1 system-auth-control enabled max-req 2
quiet-period 60 seconds re-authperiod 3600 seconds
server-timeout 30 seconds shutdown-timeout 300 seconds
supp-timeout 30 seconds tx-period 30 seconds !---
Verifies dot1x status before authentication. Cat6K>
(enable)
```

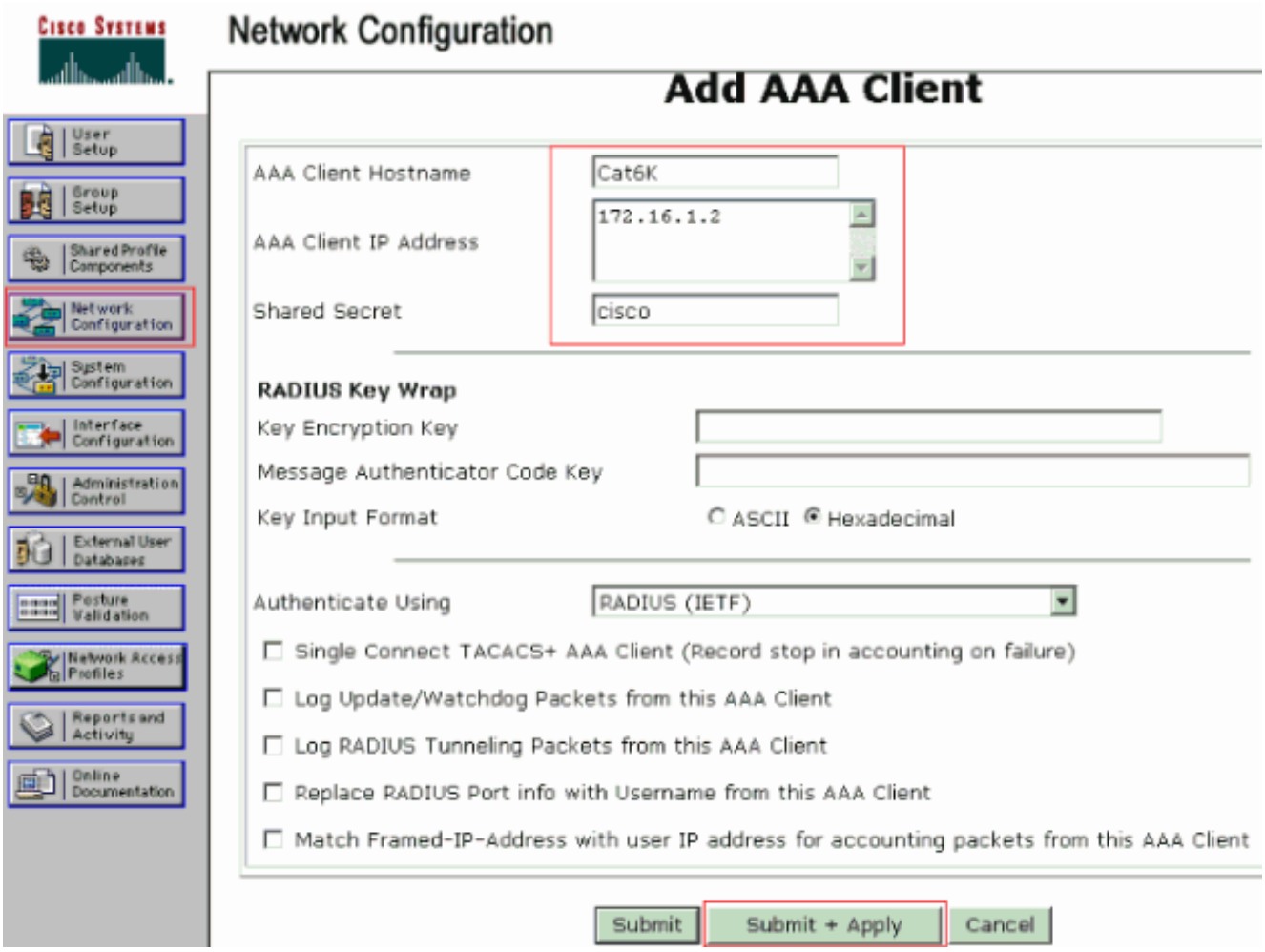
Настройка RADIUS-сервера

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

1. Для настройки клиента AAA нажмите **Network Configuration** на окне управления ACS.
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 = Интерфейс управления (sc0) IP-адрес **коммутатора (172.16.1.2)**.Общий секретный ключ = Ключ Радиуса настроен 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:

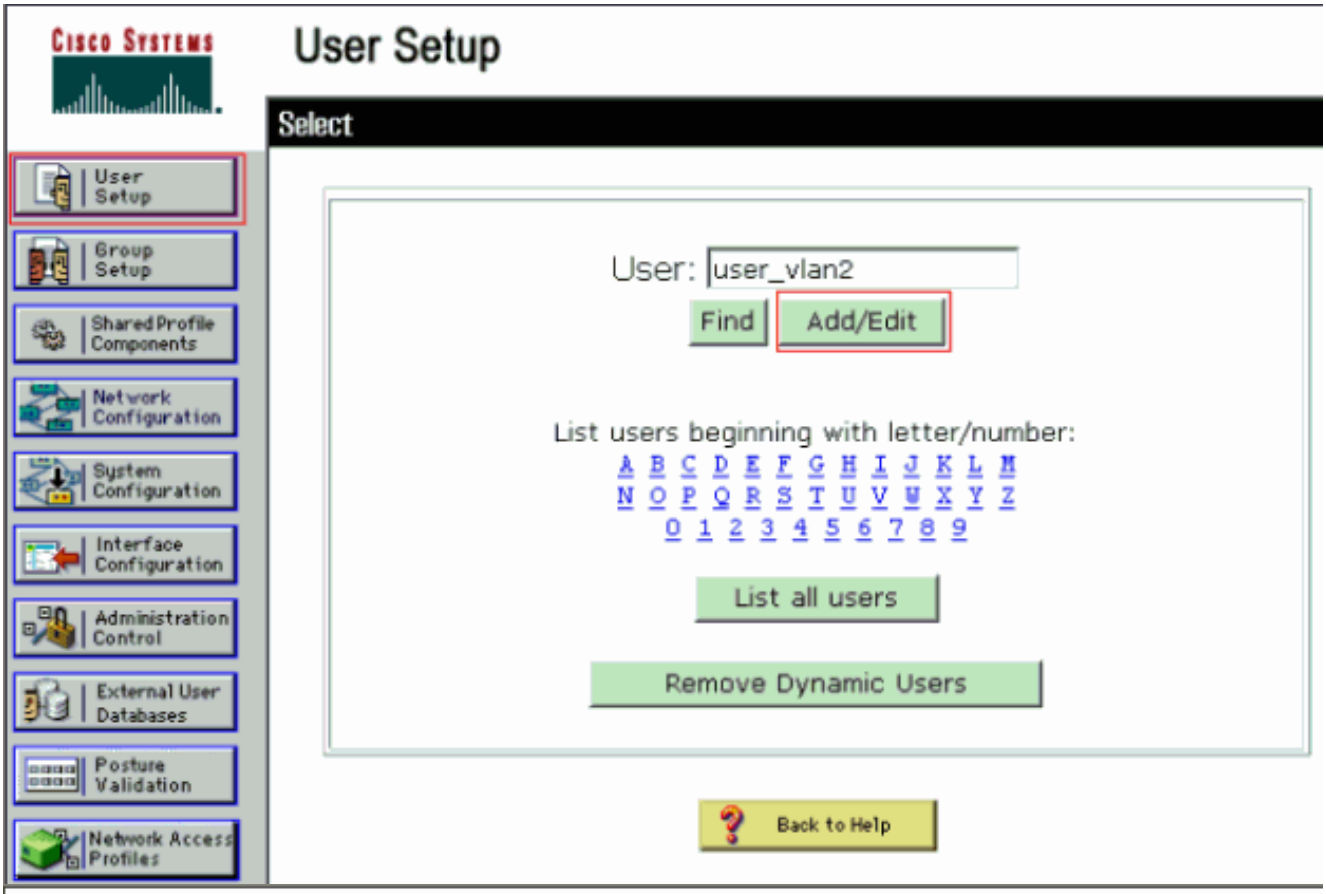


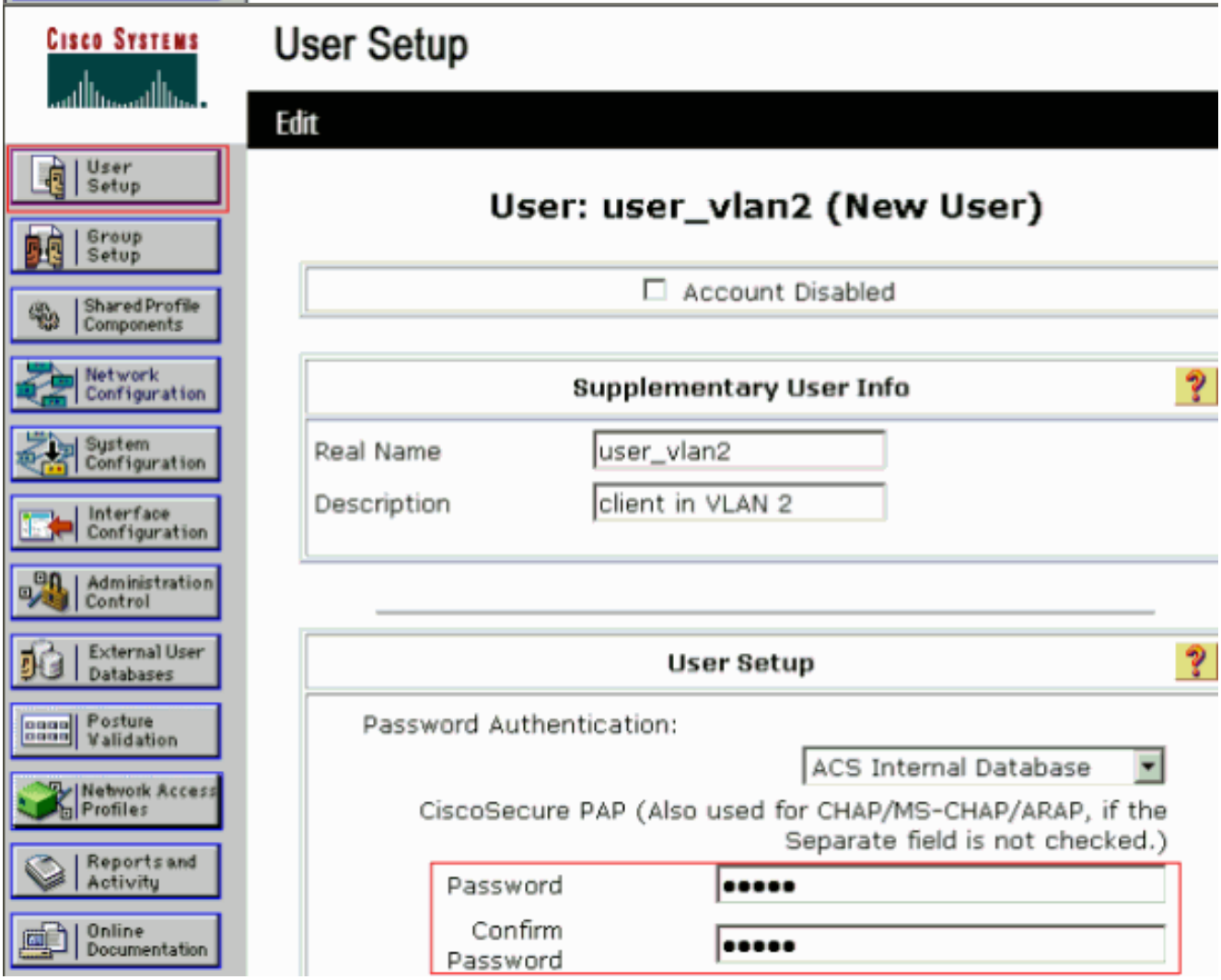
Выполните эти шаги для настройки сервера RADIUS для аутентификации, VLAN и присвоения IP-адреса:

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, соединяющихся с VLAN 2 и другим пользователем **user_vlan3** для клиентов, соединяющихся 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, завершите ту же процедуру.

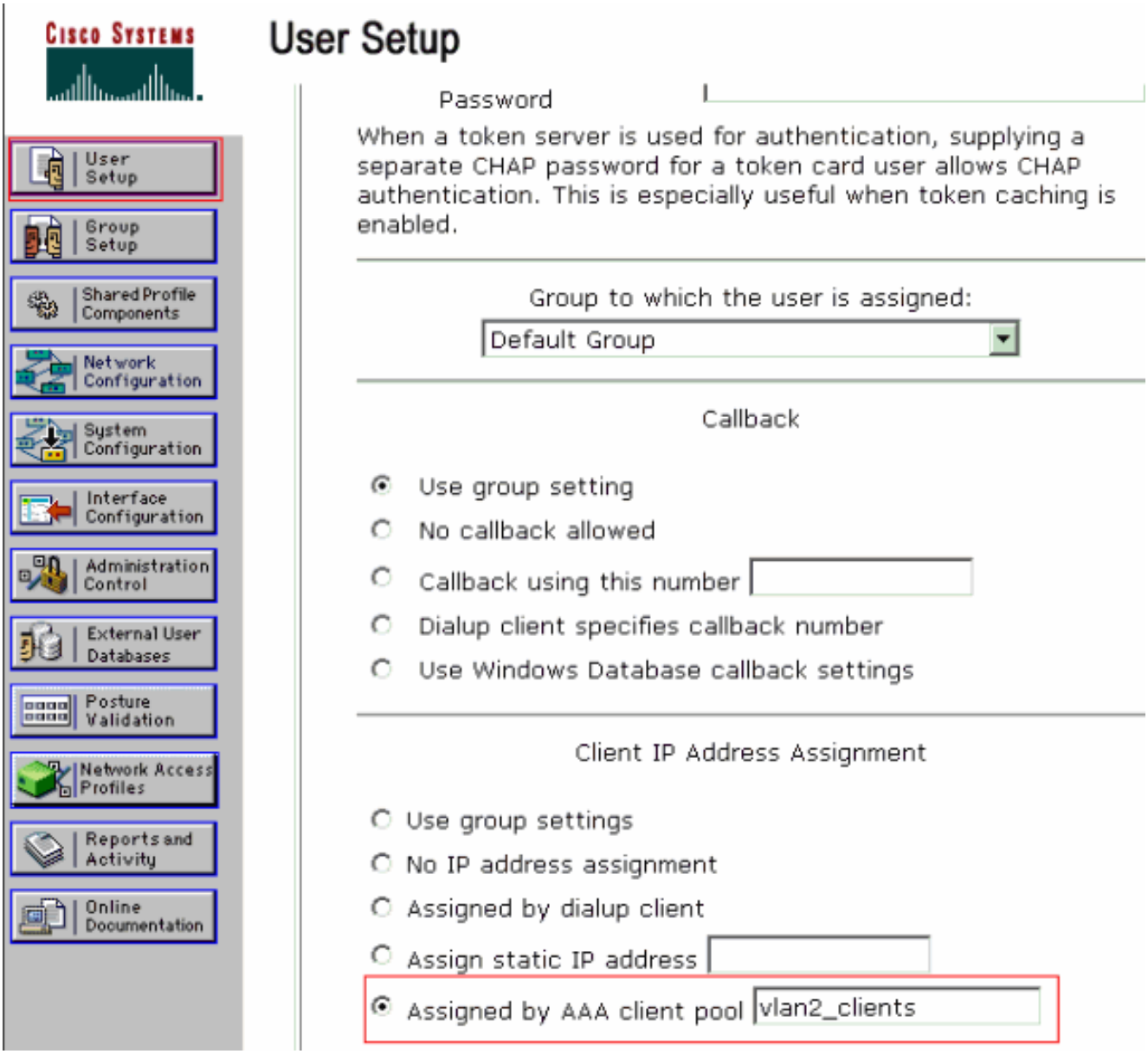
1. Чтобы добавить и настроить пользователей, нажмите **User Setup** и определите имя пользователя и
   пароль.





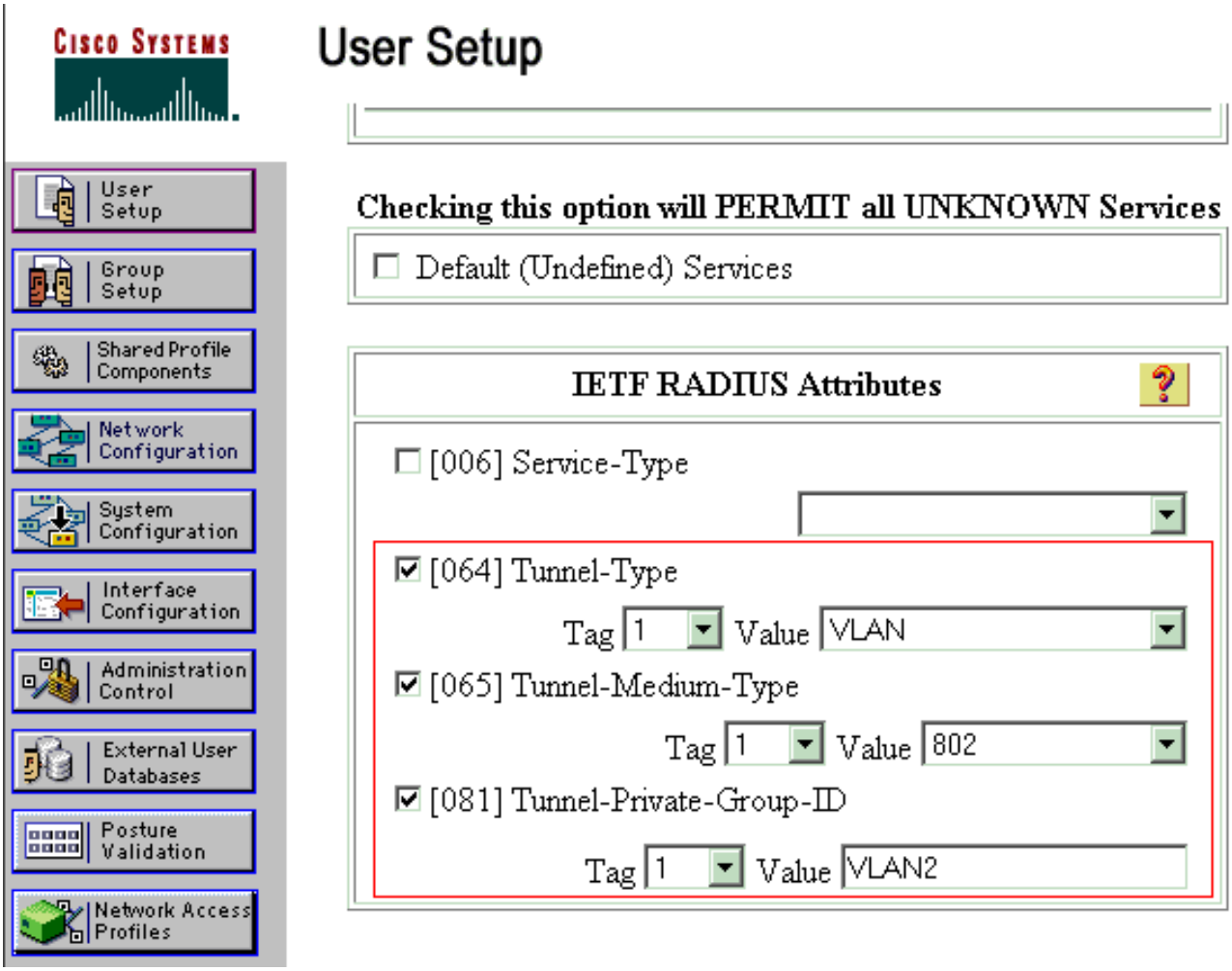
2. **Определите назначение IP-адреса клиента как Assigned by AAA client pool (назначенный из пула клиентов AAA-сервера).** Введите имя назначенного из пула IP-

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 любую метку кроме 1. Для присвоения пользователя на определенную VLAN необходимо также определить атрибут 81 с *названием* VLAN, которое соответствует.**Примечание:** *Название* VLAN должно быть точно тем же как то, настроенное в коммутаторе.**Примечание:** Назначение VLAN на основе *номера виртуальной локальной сети (VLAN)* не поддерживается с CatOS.



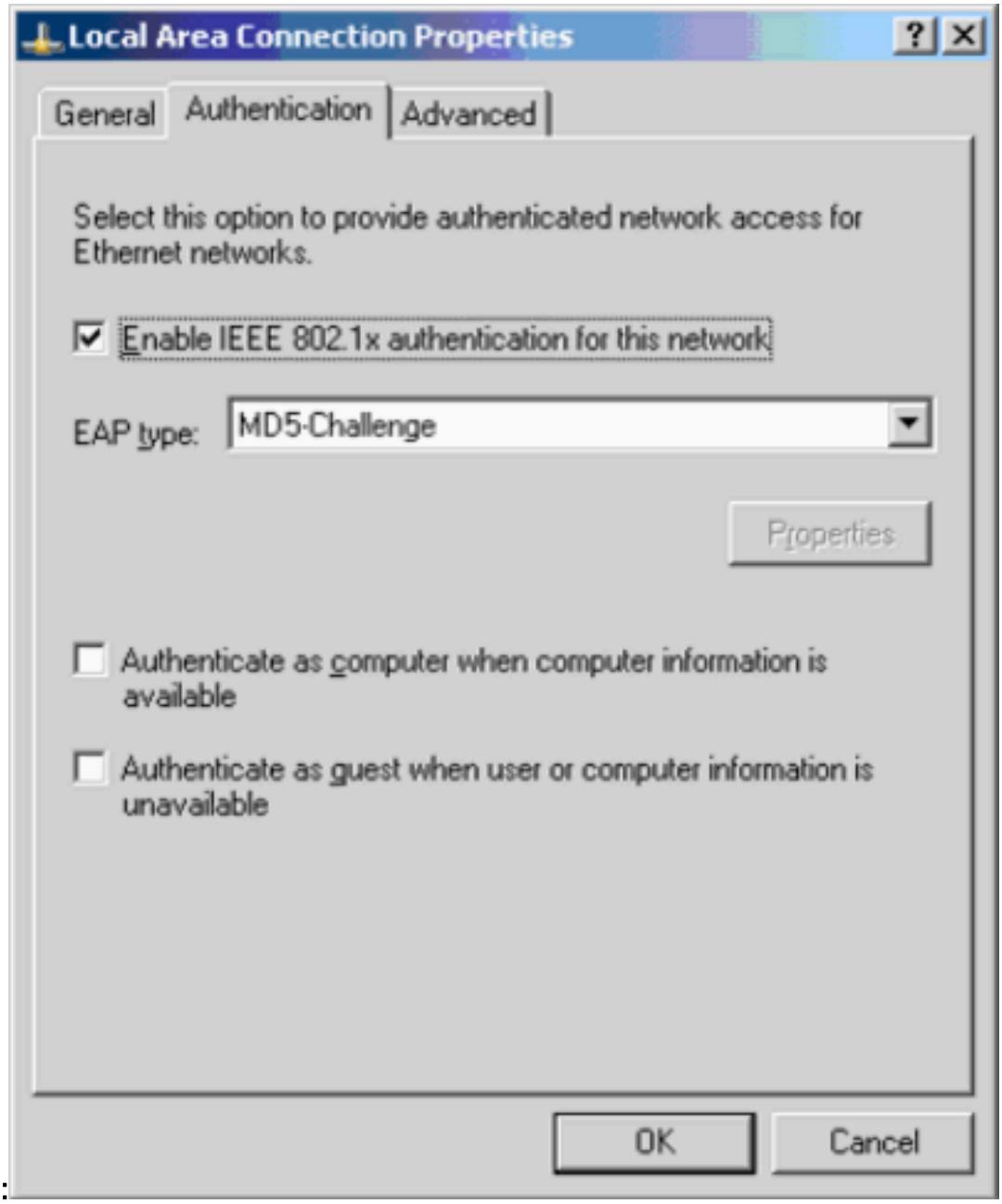
См. RFC 2868: Атрибуты RADIUS для поддержки протокола туннеля.**Примечание:** В начальной конфигурации сервера ACS атрибуты RADIUS IETF могут быть не в состоянии отображаться в **Настройке пользователя**. Выберите **Interface configuration> RADIUS (IETF)** для включения атрибутов IETF на экране пользовательской конфигурации. **Затем выполните проверку атрибутов 64, 65 и 81 в столбцах User и Group.**

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). Выполните следующие действия:

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.**

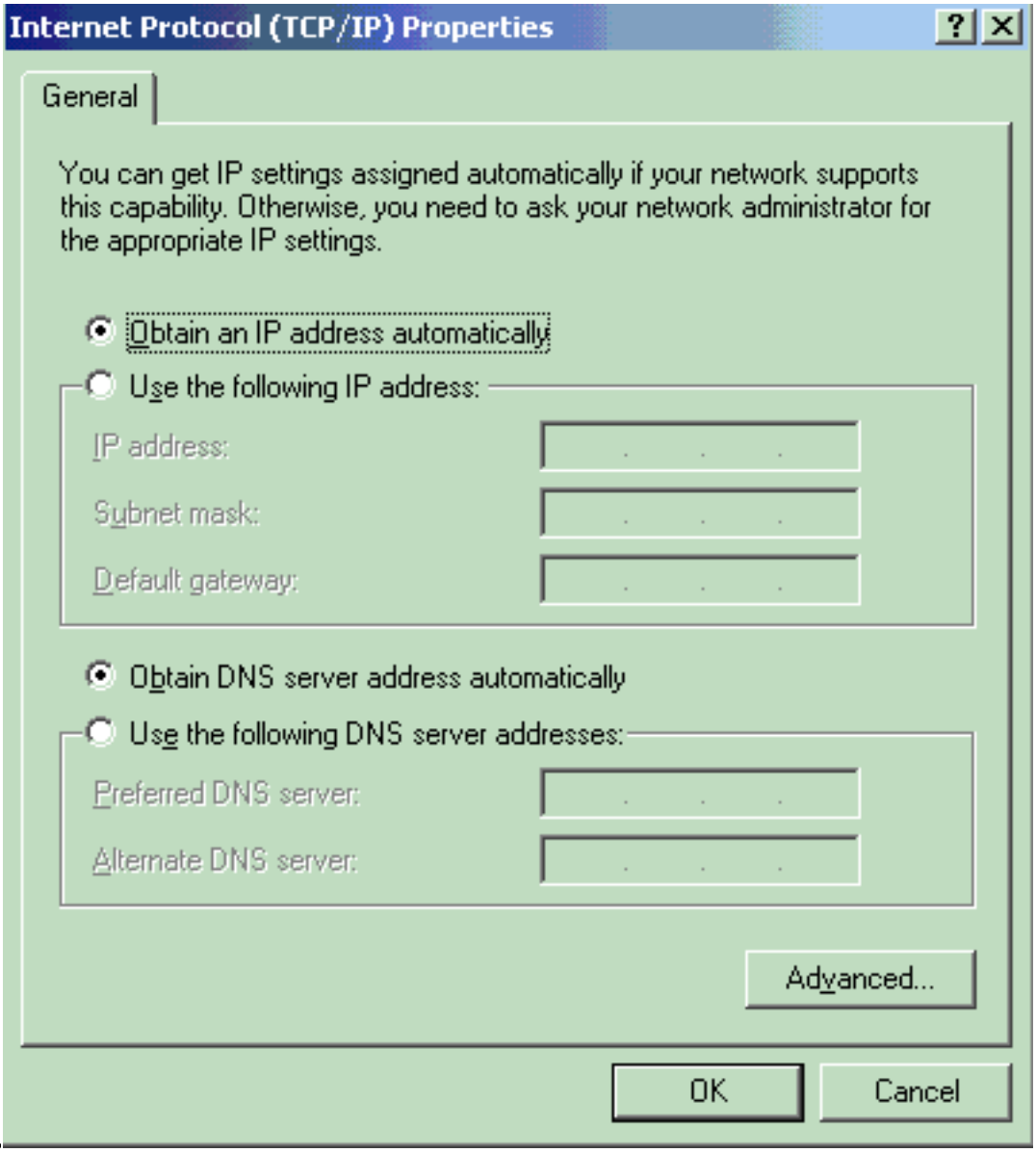
пример):



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

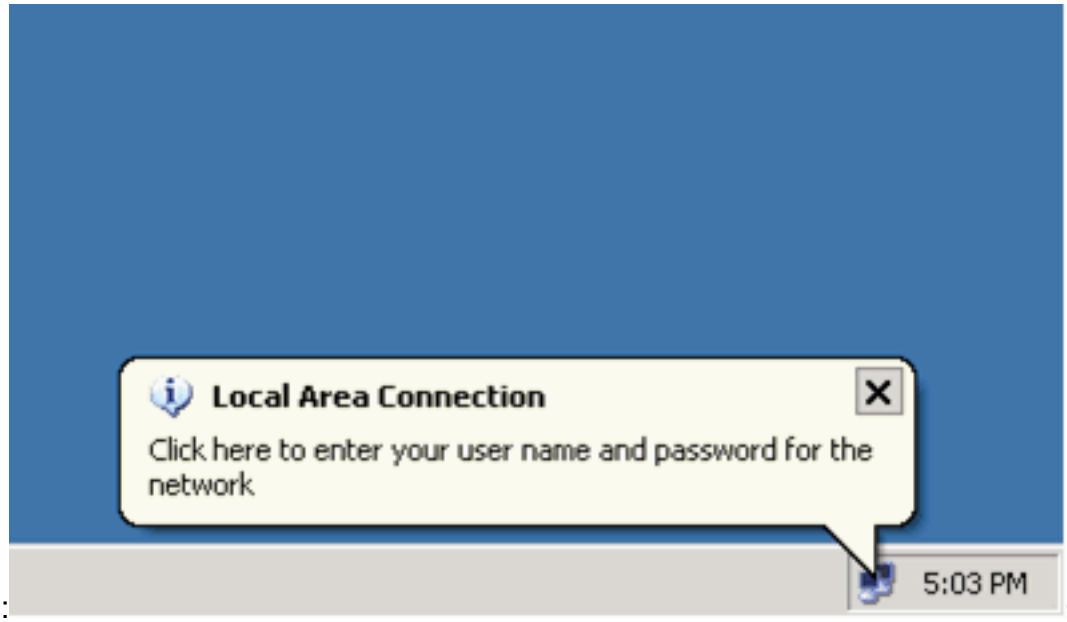
Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

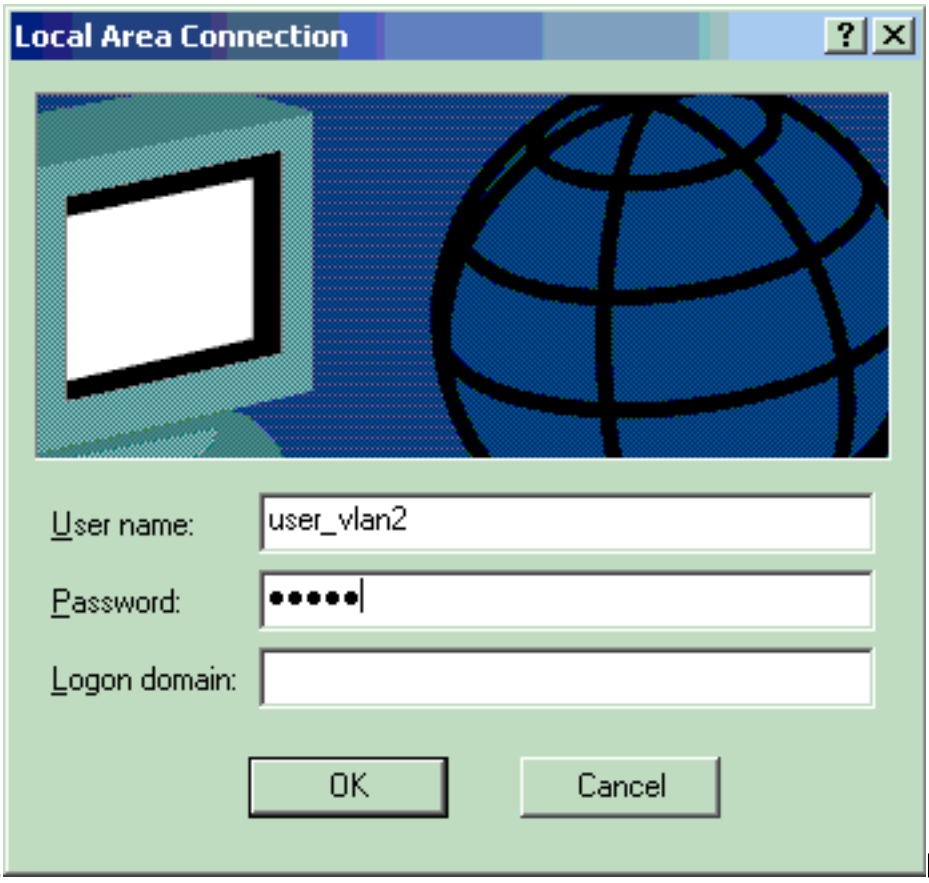
Клиентский ПК

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

1. Нажмите это предложение, как показано в

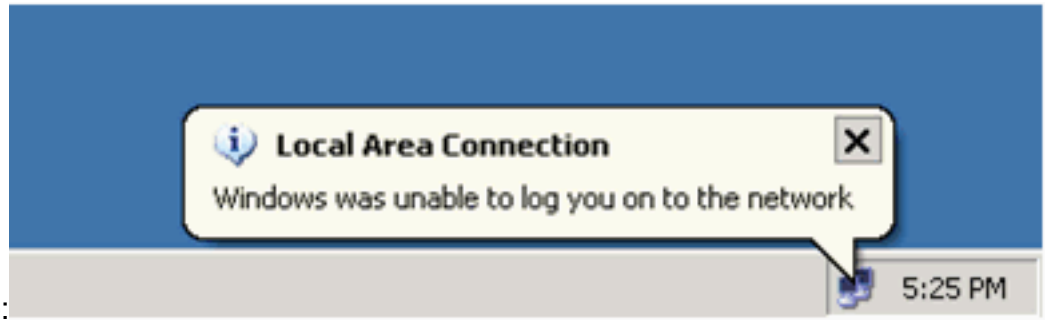
примере: 

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. В ПК 3 и 4, введите VLAN 3 учетных данных пользователя.
3. Если никакие сообщения об ошибках не появляются, проверяют подключение с обычными методами, такой как через доступ сетевых ресурсов и с **командой ping**. Это - выходные данные от ПК 1, который показывает **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> (enable) **show port dot1x 3/1-5** Port Auth-State BEnd-State Port-Control Port-Status ----- ------------------ ---------- ------------------ ------------ 3/1 **force-authorized** idle force-authorized **authorized** *!--- This is the port to which RADIUS server is connected.* 3/2 **authenticated** idle auto **authorized** 3/3 **authenticated** idle auto **authorized** 3/4 **authenticated** idle auto **authorized** 3/5 **authenticated** idle auto **authorized** Port Port-Mode Re-authentication Shutdown-timeout ----- ------------ ----------------- --- ------------ 3/1 SingleAuth disabled disabled 3/2 SingleAuth disabled disabled 3/3 SingleAuth disabled disabled 3/4 SingleAuth disabled disabled 3/5 SingleAuth disabled disabled` Проверьте состояние VLAN после успешной аутентификации.`Cat6K> (enable) **show vlan** VLAN Name Status IfIndex Mod/Ports, Vlans ---- -------------------------------- - -------- ------- ----------------------- 1 default active 6 2/1-2 3/6-48 **2 VLAN2 active 83 3/2-3 3 VLAN3 active 84 3/4-5** 4 AUTHFAIL_VLAN active 85 5 GUEST_VLAN active 86 10 RADIUS_SERVER active 87 3/1 1002 fddi-default active 78 1003 token-ring-default active 81 1004 fddinet-default active 79 1005 trnet-default active 80 *!--- Output suppressed.*`
2. Проверьте статус привязки к DHCP от модуля маршрутизации (MSFC) после успешной аутентификации.`Router#**show ip dhcp binding** IP address Hardware address Lease expiration Type 172.16.2.2 0100.1636.3333.9c Feb 14 2007 03:00 AM Automatic 172.16.2.3 0100.166F.3CA3.42 Feb 14 2007 03:03 AM Automatic 172.16.3.2 0100.145e.945f.99 Feb 14 2007 03:05 AM Automatic 172.16.3.3 0100.1185.8D9A.F9 Feb 14 2007 03:07 AM Automatic`

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Пример настройки аутентификации по стандарту IEEE 802.1x с использованием Catalyst 6500/6000 с ПО Cisco IOS
- Инструкции по развертыванию коммутатора Catalyst и ACS
- Спецификация RFC 2868: Атрибуты RADIUS для поддержки туннельного протокола
- Настройка параметров аутентификации 802.1x
- Страницы поддержки продуктов LAN
- Страница поддержки коммутационных решений для локальной сети
- Cisco Systems – техническая поддержка и документация