VSA Airespace Cisco на примере конфигурации сервера RADIUS Microsoft IAS

Содержание

Введение

Этот документ показывает вам, как настроить сервер Microsoft Internet Authentication Service (IAS) для поддержки Airespace Cisco Определяемые поставщиком Атрибуты (VSA). Код поставщика для VSA Airespace Cisco **14179**.

Предварительные условия

Требования

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

- Знание того, как настроить сервер IAS
- Знание конфигурации Облегченных точек доступа (LAP) и контроллеры беспроводной локальной сети Cisco (WLC)
- Знание решений по обеспечению безопасности унифицированной беспроводной связи Cisco

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- Сервер Microsoft Windows 2000 с IAS
- WLC Cisco 4400, который работает под управлением ПО версии 4.0.206.0
- Облегченные точки доступа Cisco 1000 серии
- Беспроводной клиентский адаптер a/b/g 802.11 с микропрограммным обеспечением 2.5
- Набор программ Aironet Desktop Utility версии 2.5

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.

Примечание: Этот документ предназначен, чтобы дать читателю пример на конфигурации, требуемой на сервере IAS поддерживать VSA Airespace Cisco. Конфигурация сервера IAS, представленная в этом документе, была протестирована в лабораторной работе и работает как ожидалось. При наличии затруднений при настройке сервера IAS свяжитесь с Microsoft для справки. Центр технической поддержки Cisco не поддерживает конфигурацию Microsoft Windows server.

Этот документ предполагает, что WLC настроен для главной операции и что LAP зарегистрированы к WLC. Если вы - новый пользователь, пытающийся устанавливать WLC для главной операции с LAP, обратитесь к регистрации облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC).

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

В большей части беспроводной локальной сети (WLAN) системы каждый WLAN имеет статическую политику, которая применяется ко всем клиентам, привязанным к идентификатору набора сервисов (SSID). Будучи достаточно мощным, этот способ имеет ряд ограничений, поскольку он требует связывания клиентов с различным идентификаторами SSID для наследования разных политик QoS и безопасности.

Однако идентификационные сети Поддержки решений беспроводной сети LAN Cisco, которые позволяют сети объявлять одиночный SSID и определенных пользователей для наследования другого QoS или политики безопасности на основе их профилей пользователей. Определенная политика, что можно управлять идентификационными сетями использования, включает:

- **Качество обслуживания** — Когда подарок в ДОСТУПЕ К СЕРВЕРУ RADIUS Принимают, значение Уровня QoS, отвергает значение QoS, заданное в профиле WLAN.
- **ACL** — Когда атрибут Списка контроля доступа (ACL) присутствует в ДОСТУПЕ К СЕРВЕРУ RADIUS, Принимает, система применяет Название ACL к станции клиента после того, как это аутентифицируется. Это отвергает любые ACL, которые назначены на интерфейс.
- **VLAN** — Когда Interface-Name VLAN или ТЕГ VLAN присутствуют в ДОСТУПЕ К

СЕРВЕРУ RADIUS, Принимает, система размещает клиента в определенный интерфейс.

- **ИДЕНТИФИКАТОР WLAN** — Когда атрибут ИДЕНТИФИКАТОРА WLAN присутствует в ДОСТУПЕ К СЕРВЕРУ RADIUS, Принимает, система применяет ИДЕНТИФИКАТОР WLAN (SSID) к станции клиента после того, как это аутентифицируется. ИДЕНТИФИКАТОР WLAN передается WLC во всех экземплярах аутентификации кроме IPSec. В случае web-аутентификации, если WLC получает атрибут ИДЕНТИФИКАТОРА WLAN в ответе на аутентификацию от AAA-сервера, и это не совпадает с ID WLAN, аутентификация отклонена. Другие типы методов безопасности не делают этого.
- **DSCP-значение** — Когда подарок в ДОСТУПЕ К СЕРВЕРУ RADIUS Принимают, DSCP-значение, отвергает DSCP-значение, заданное в профиле WLAN.
- **802.1p-метка** — Когда подарок в ДОСТУПЕ К СЕРВЕРУ RADIUS Принимают, 802.1p значение, отвергает по умолчанию, заданный в профиле WLAN.

Примечание: Функция VLAN только поддерживает фильтрацию по MAC-адресам, 802.1X и Защищенный доступ по протоколу Wi-Fi (WAP). Функция VLAN не поддерживает web-аутентификацию или IPSec. База данных Фильтра локального MAC - адреса операционной системы была расширена для включения имени интерфейса. Это позволяет фильтрам локального MAC - адреса задавать, какой интерфейс клиенту нужно назначить. Отдельный сервер RADIUS может также использоваться, но сервер RADIUS должен быть определен с помощью Меню системы безопасности.

См. Идентификационные Сети Настройки для получения дополнительной информации об идентификационных сетях.

Настройте IAS для VSA Airespace

Для настройки IAS для VSA Airespace необходимо выполнить эти шаги:

1. Настройте WLC как клиента AAA на IAS
2. Настройте политику удаленного доступа по IAS

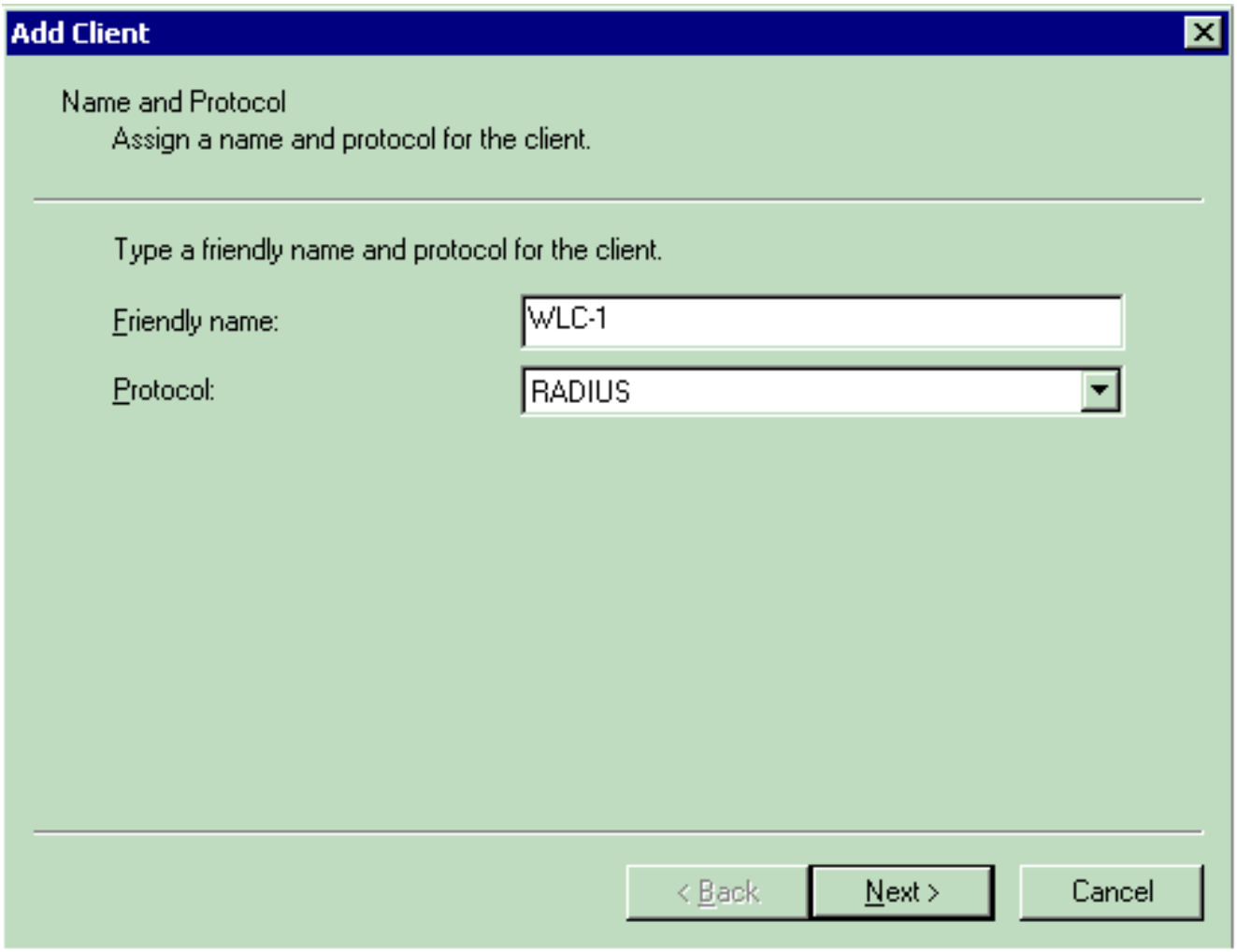
Примечание: VSA настроены под Политикой Удаленного доступа.

Настройте WLC как клиента AAA на IAS

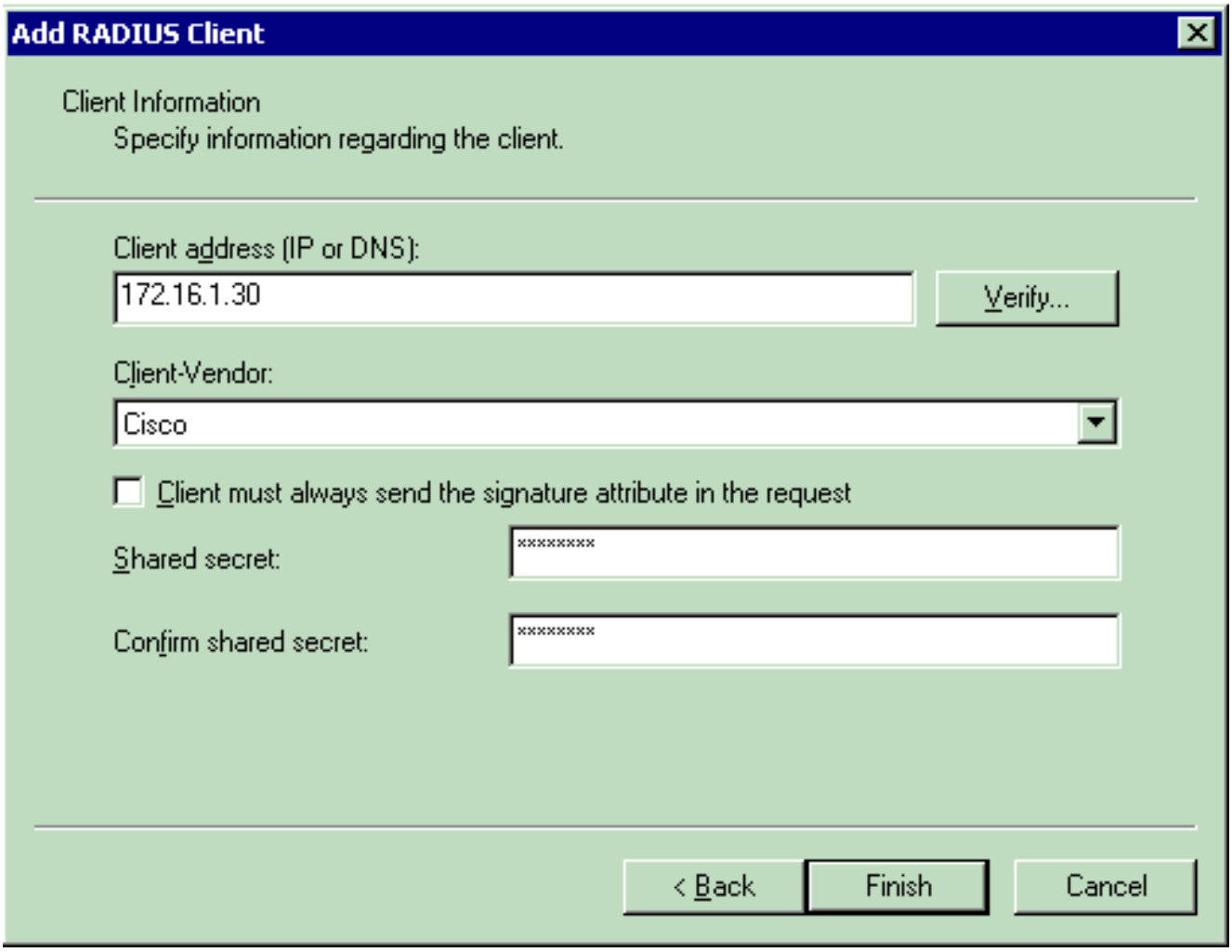
Выполните эти шаги для настройки WLC как клиент AAA на IAS:

1. Нажмите **Programs> Administrative Tools> Internet Authentication Service** для запуска IAS на Microsoft 2000
   Server.

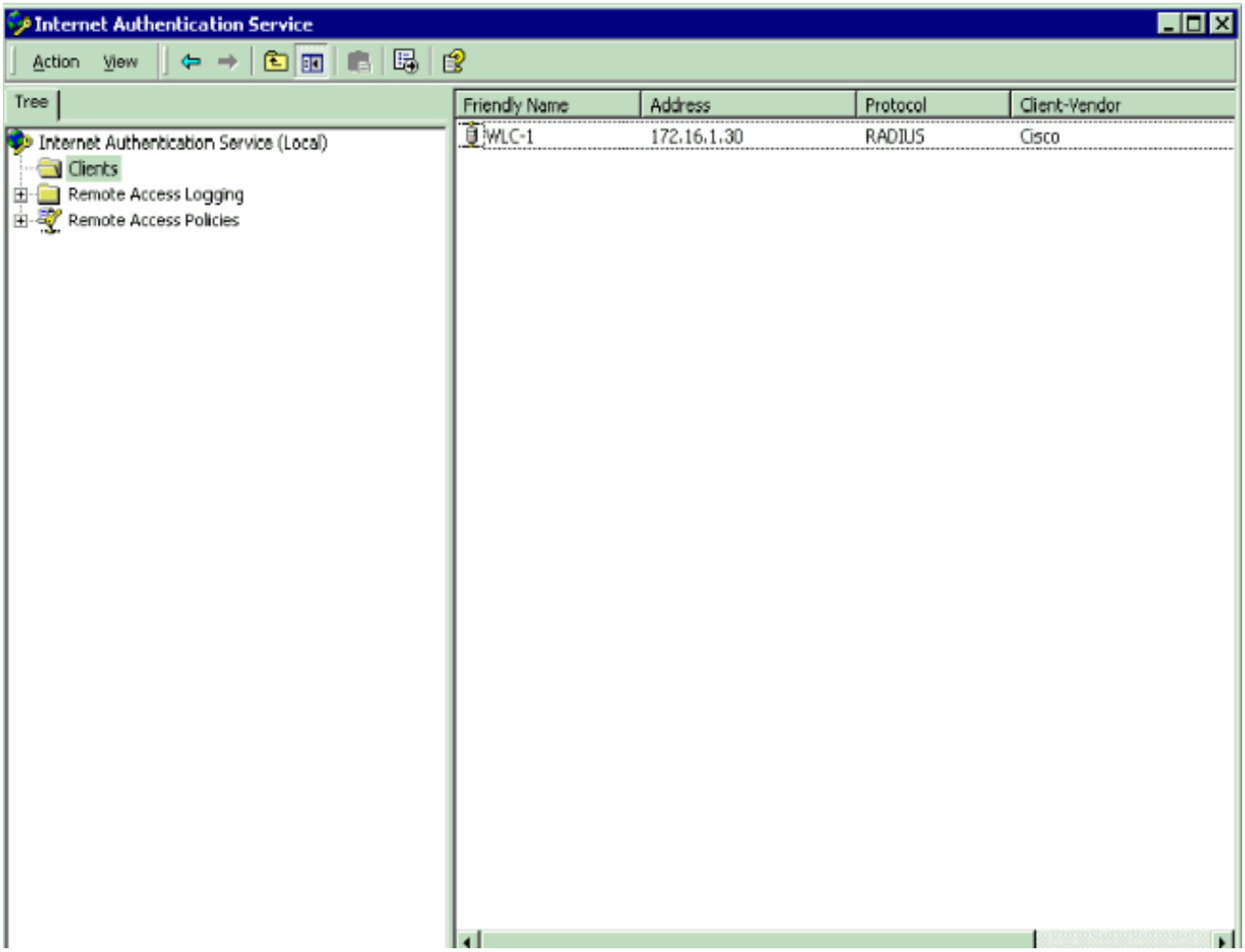
2. Щелкните правой кнопкой мыши папку **Clients** и выберите **New Client** для добавления нового Клиента RADIUS.
3. В Окне клиента Add введите имя клиента и выберите **RADIUS** в качестве Протокола. **Нажмите кнопку Next.**В данном примере имя клиента является *WLC-1*.**Примечание:** По умолчанию протокол установлен в
RADIUS.



4. В окне Add RADIUS Client введите **IP-адрес клиента**, **Клиента - поставщика** и **Общий секретный ключ**. После ввода сведений о клиенте нажмите **Finish**.Данный пример показывает клиенту, названному *WLC-1* с IP-адресом *172.16.1.30*, Клиент - поставщик установлен в *Cisco*, и Общий секретный ключ является *cisco123*:



С этой информацией WLC назвал WLC-1, добавлен как клиент AAA сервера IAS.

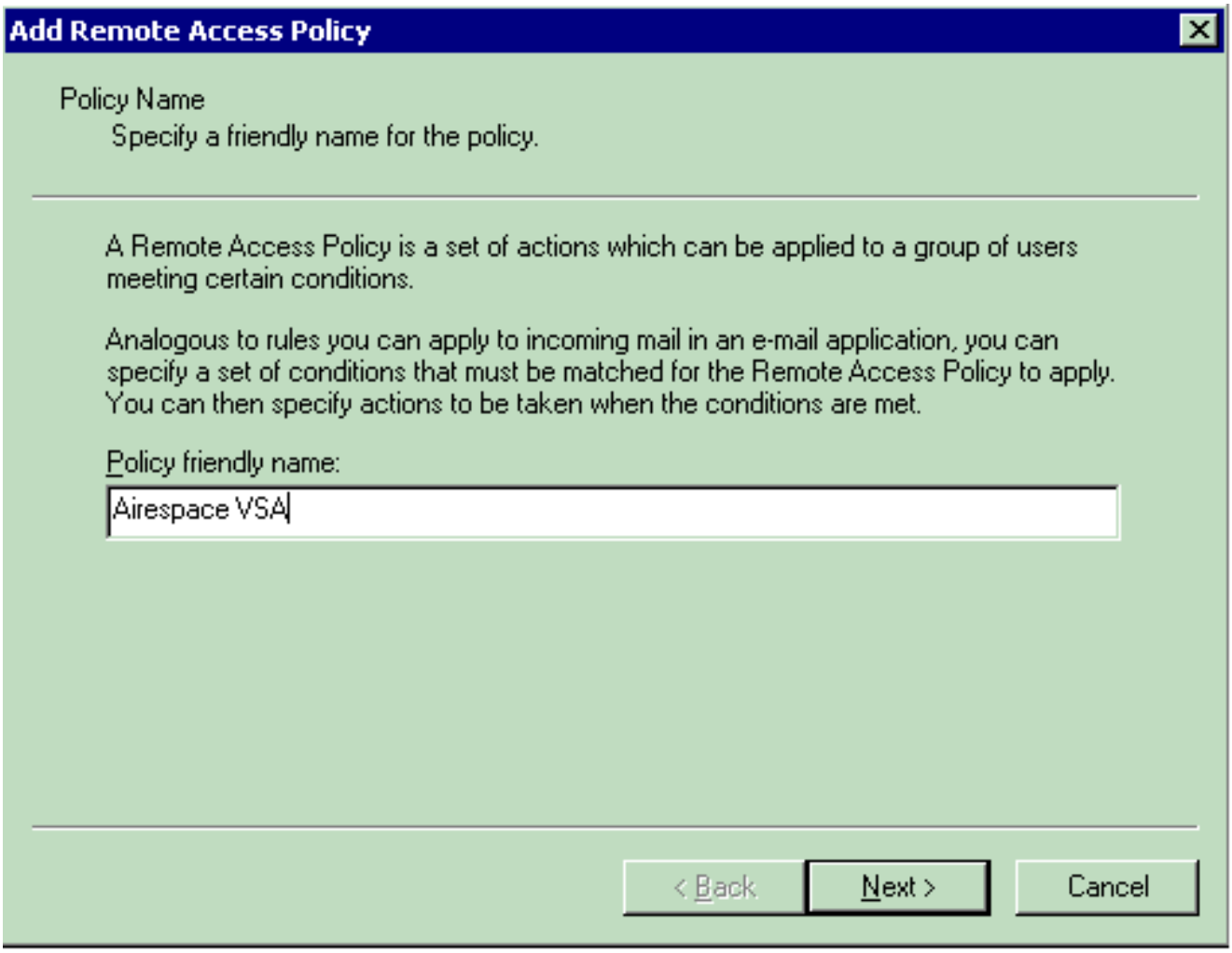


Следующий шаг должен создать Политику Удаленного доступа и настроить VSA.

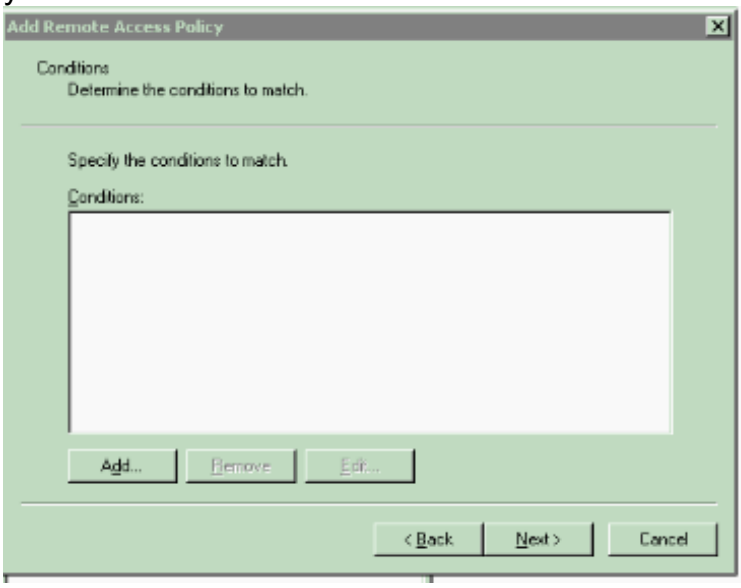
Настройте политику удаленного доступа по IAS

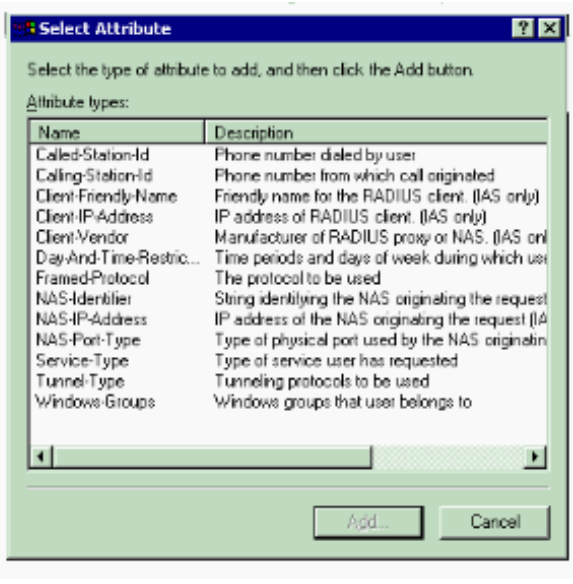
Выполните эти шаги для настройки новой Политики Удаленного доступа по IAS:

1. Щелкните правой кнопкой мыши **Политику Удаленного доступа** и выберите **New Remote AcceMSss Policy**.Окно имени Policy появляется.
2. Введите имя политики и нажмите **Next**.

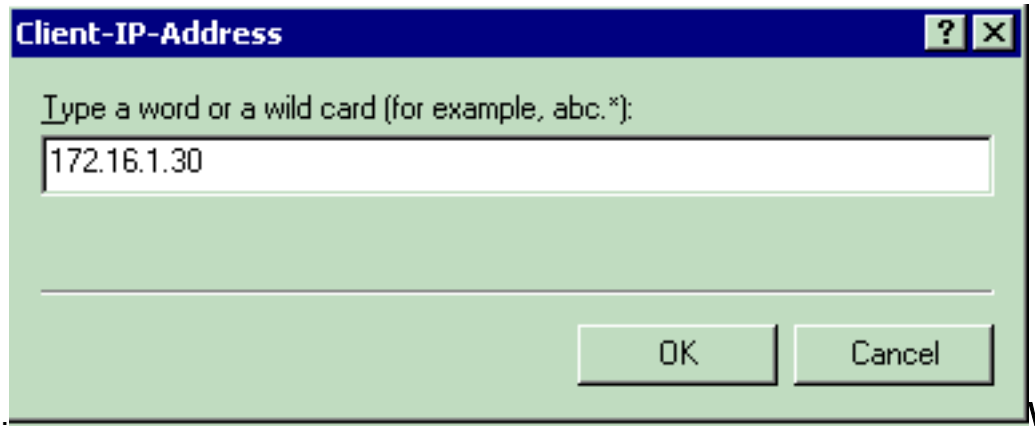


3. В следующем окне выберите условия, для которых применится Политика Удаленного доступа. **Нажмите Add** для выбора условий.

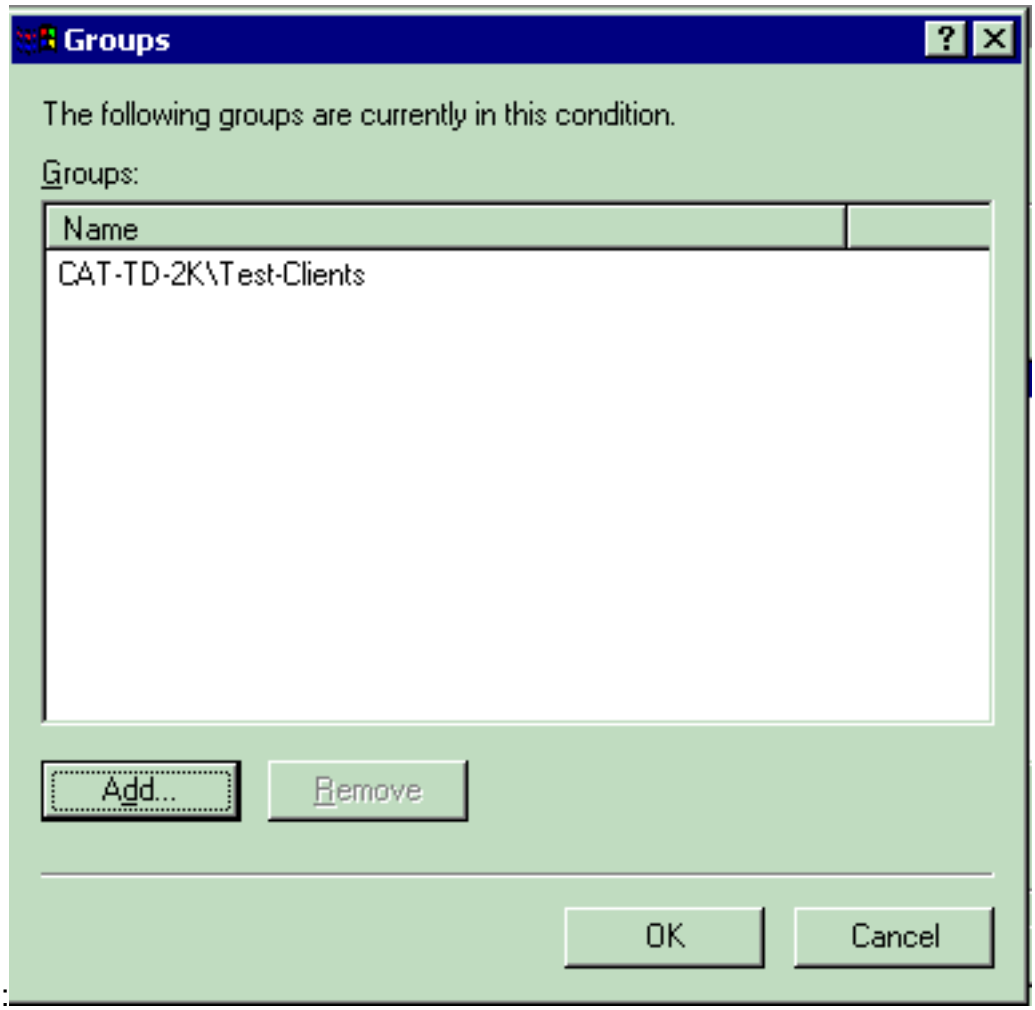




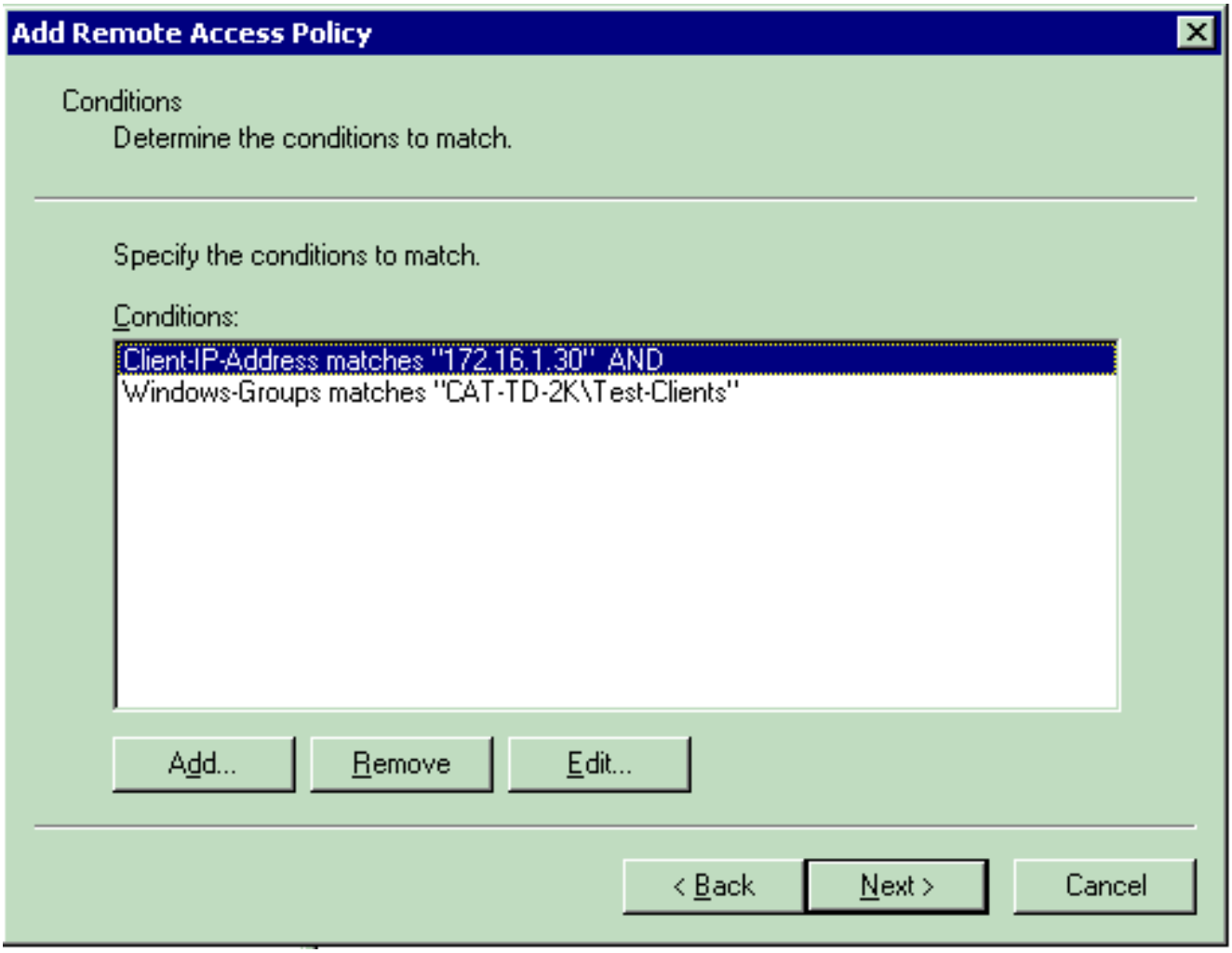
4. Из меню Типов атрибутов выберите эти атрибуты:**IP-адрес клиента** — Вводит IP-адрес клиента AAA. В данном примере введен IP-адрес WLC так, чтобы политика применилась к пакетам от



WLC. **Windows Groups** — Выберите группу Windows (группа пользователей), для которого применится политика.

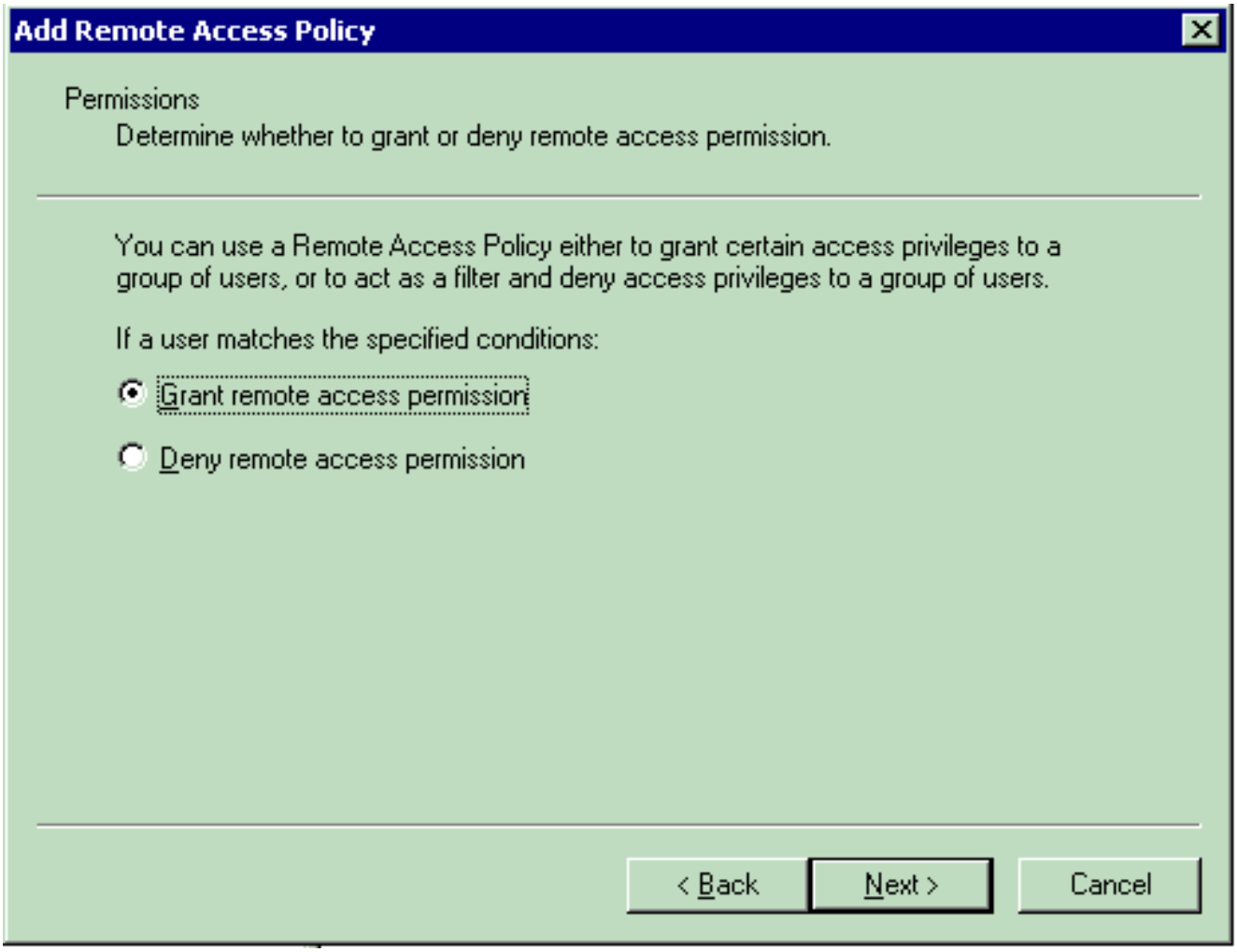


Например:

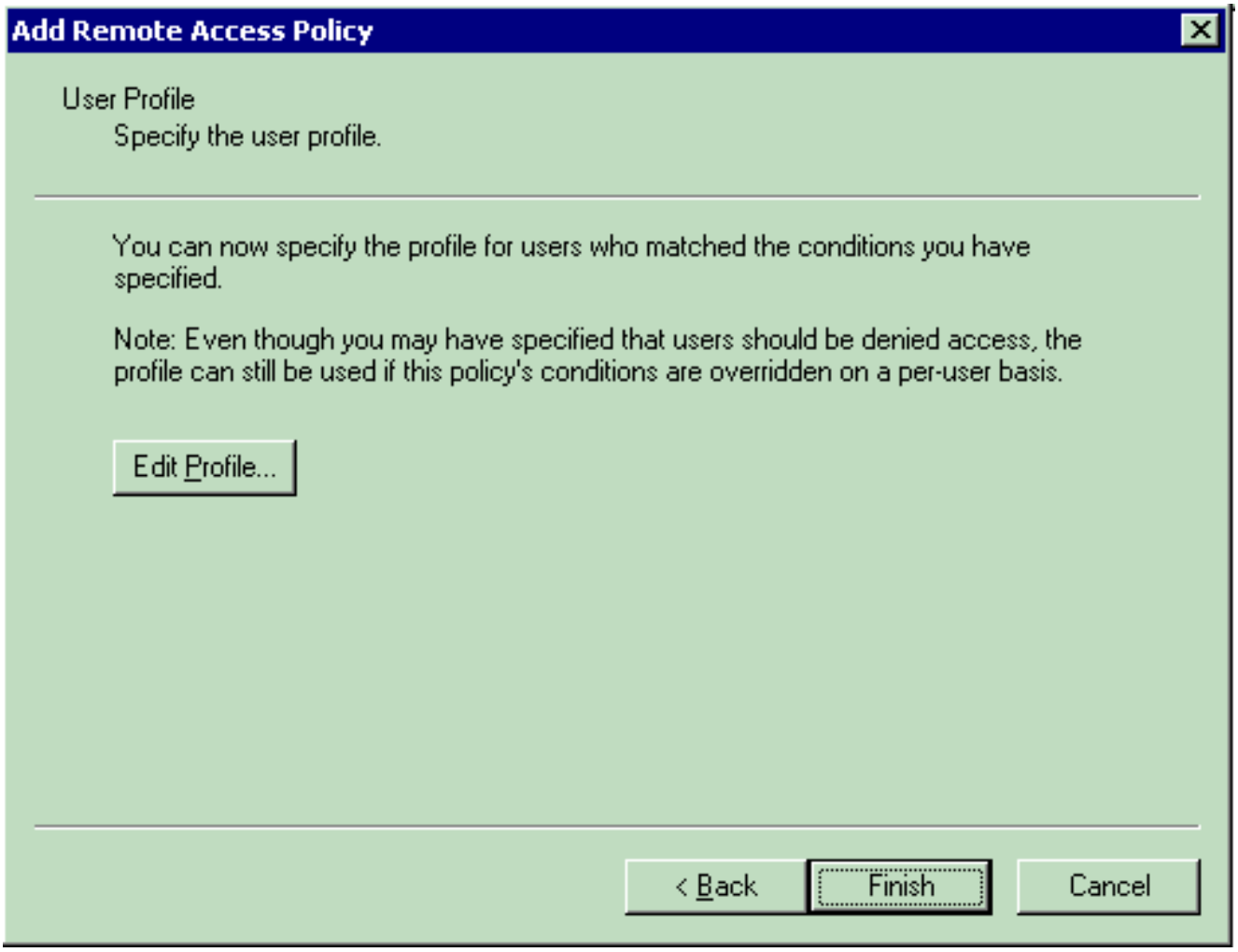


Данный пример показывает только два условия. Если существуют большие условия, добавьте те условия также и нажмите **Next**.Окно Permissions появляется.

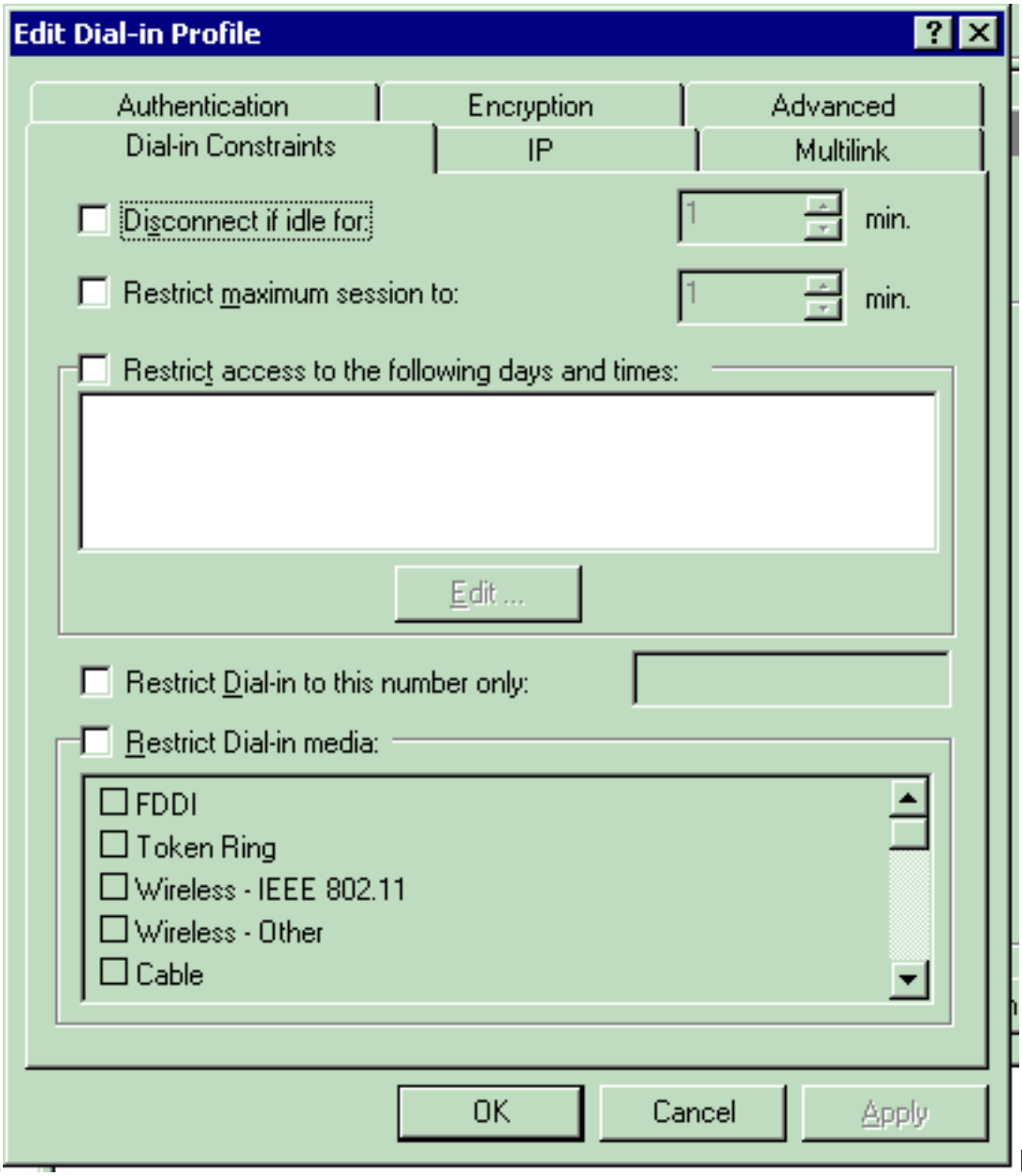
5. В окне Permissions выберите**, дают разрешение удаленного доступа**.После выбора этой опции пользователю предоставляют доступ, предоставил пользовательские соответствия указанные условия (от шага 2).



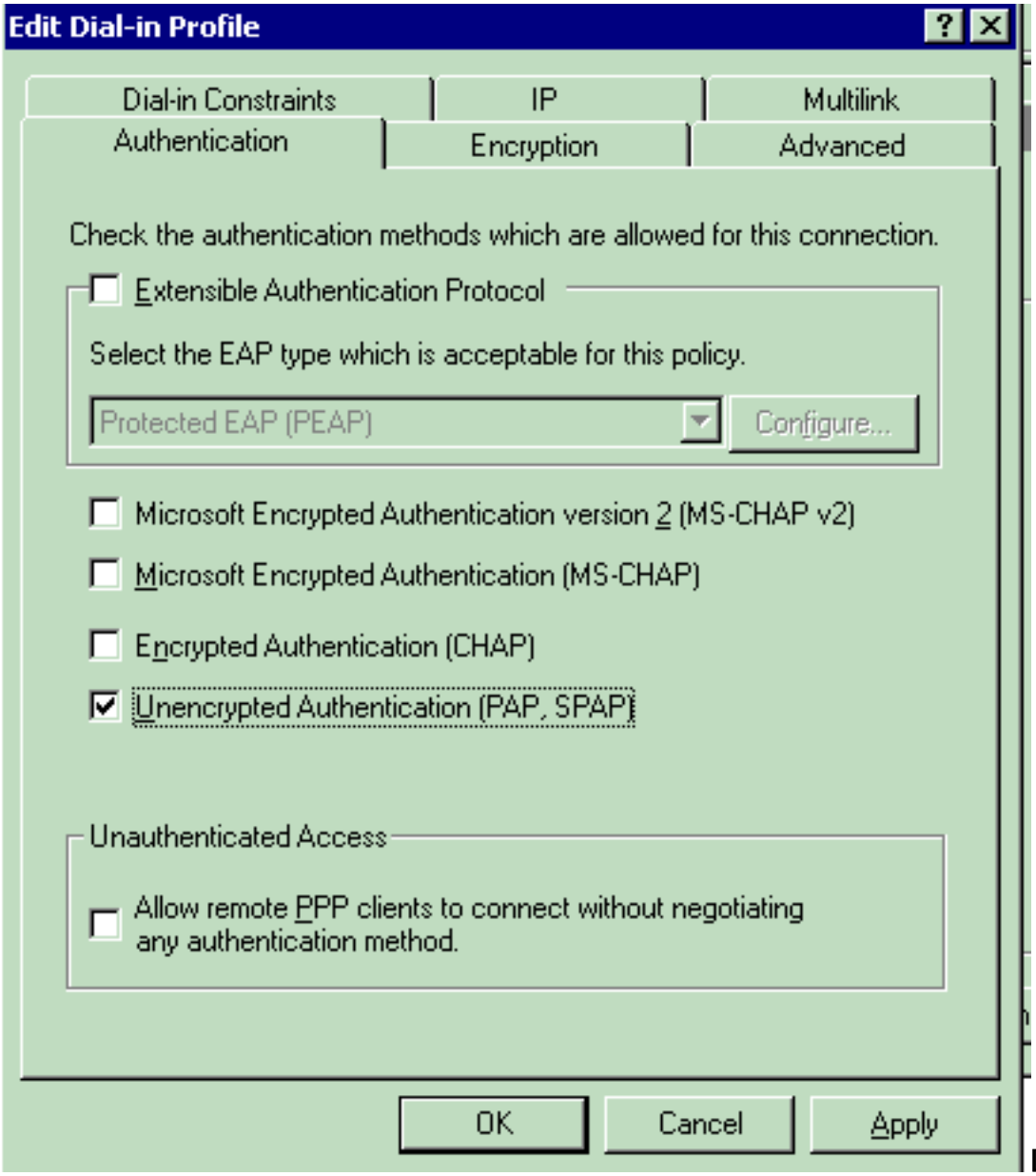
6. **Нажмите кнопку Next.**
7. Следующий шаг должен установить профиль пользователя.Даже при том, что вы, возможно, указали, что пользователи должны быть запрещены или предоставленный доступ на основе условий, профиль может все еще использоваться, если условия этой политики отвергнуты на основе для каждого пользователя.



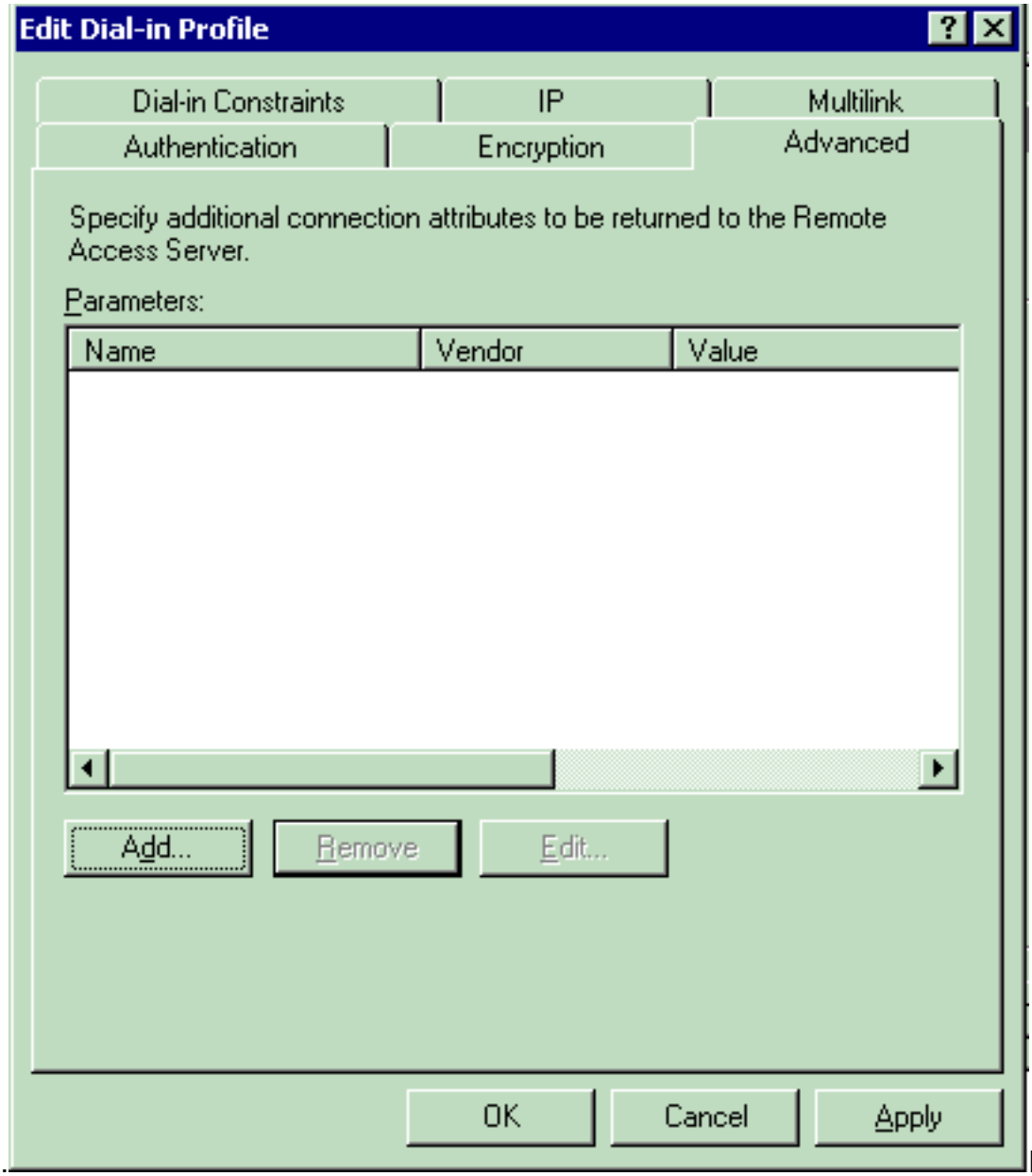
Для настройки профиля пользователя нажмите **Edit Profile** на окне User Profile.Окно Profile Наборного (телефонный) доступа Редактирования



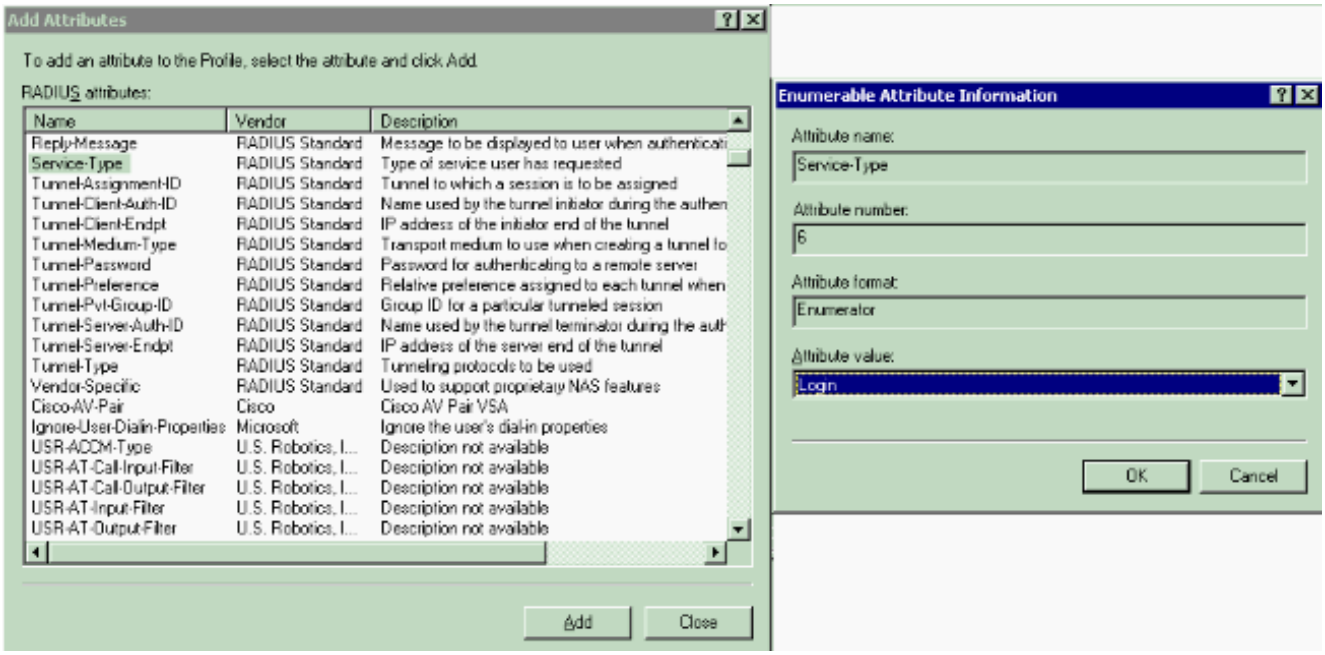
появляется. На жмите **вкладку Authentication**, затем выберите метод аутентификации, который используется в WLAN.Данный пример использует Незашифрованную проверку подлинности (PAP,



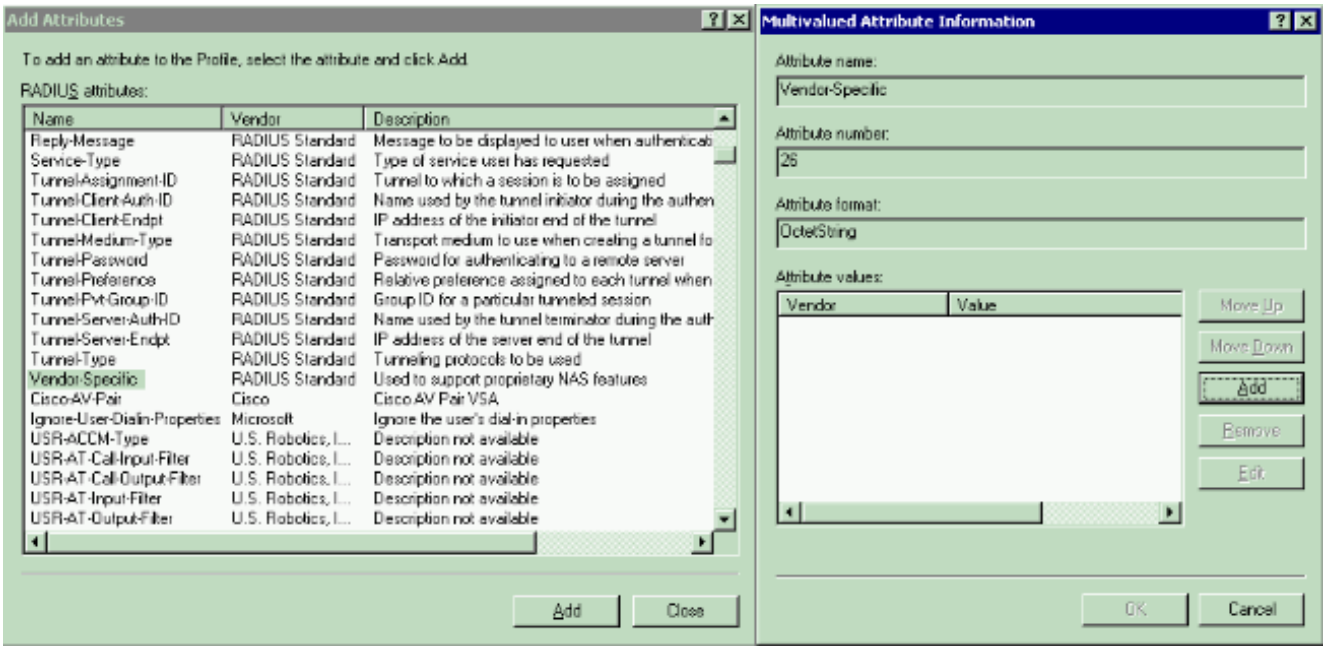
SPAP). **Щелкните вкладку Advanced ("Дополнительно").** Удалите все параметры по умолчанию и **нажмите**



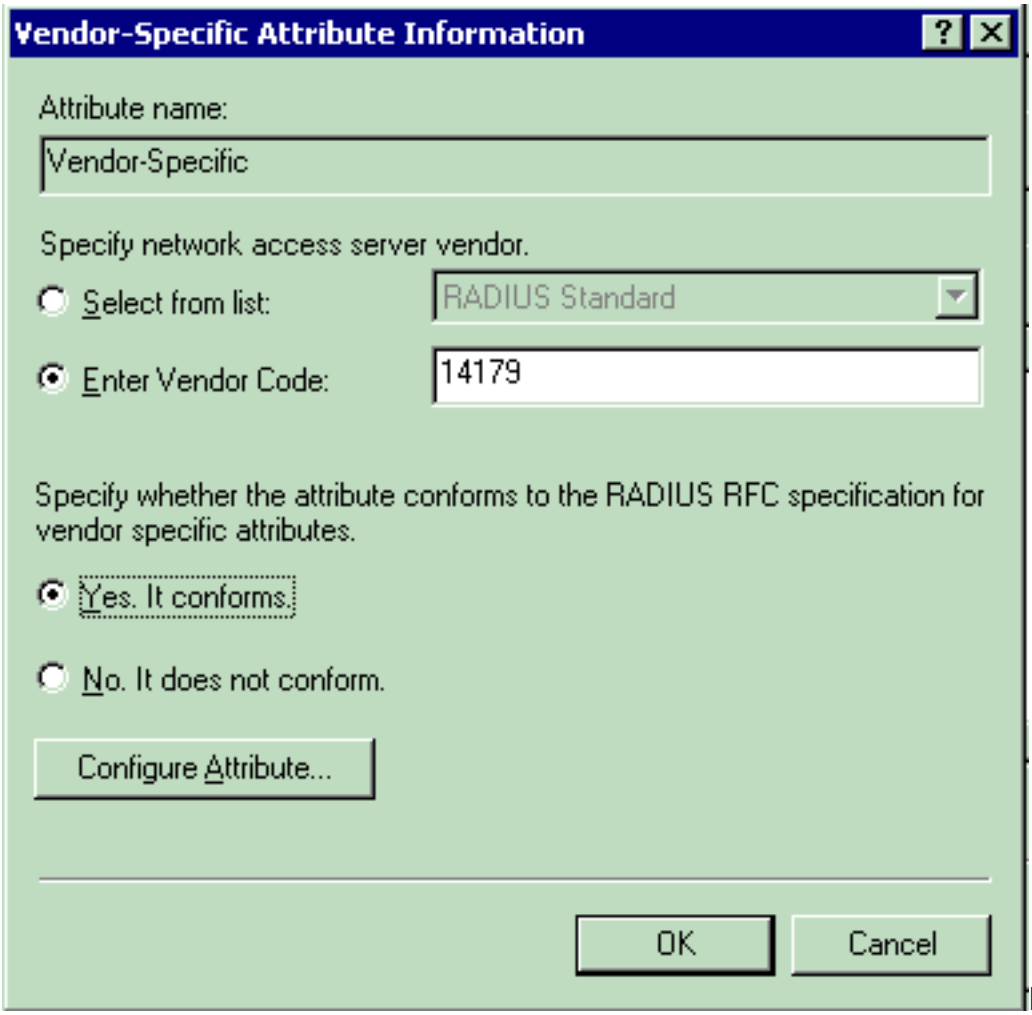
Add.Из окна **Add Attributes** выберите **Service-Type**, затем выберите значение **Входа в систему** из следующего
окна.



Затем, необходимо выбрать **Vendor-Specific attribute** из списка атрибутов RADIUS.

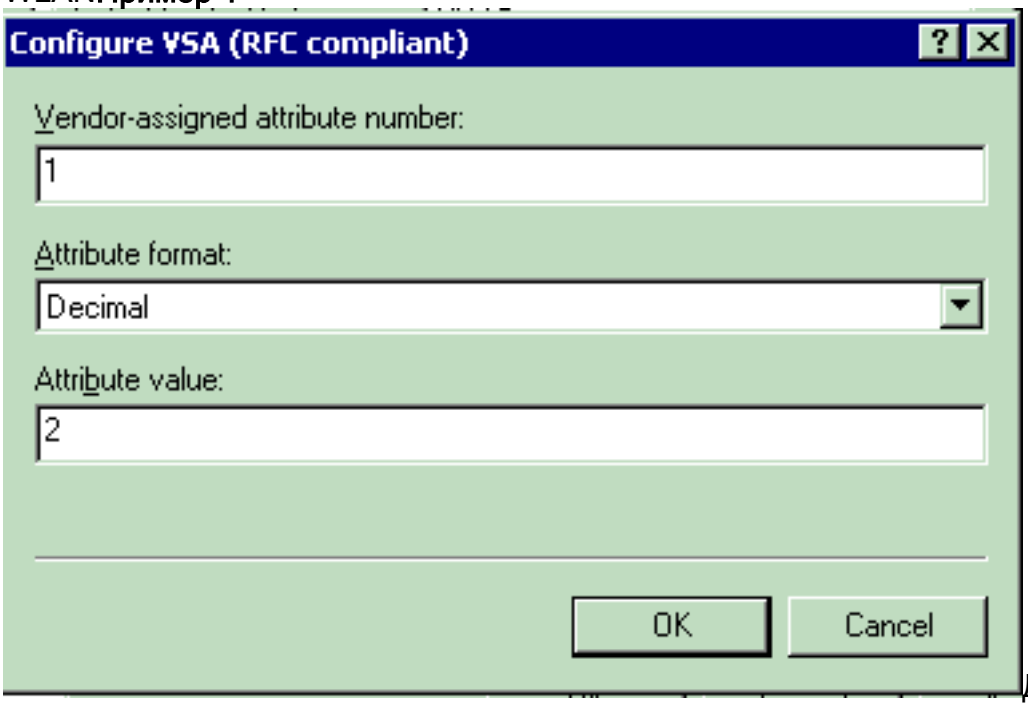


В следующем окне **нажмите Add** для выбора нового VSA.Определяемое производителем характеристика Информационное окно появляется.Под Задают поставщика сервера доступа к сети, выбирают **Enter Vendor Code**.Введите Код поставщика для VSA Airespace. Код поставщика для VSA Airespace Cisco **14179**.Поскольку этот атрибут соответствует спецификации RFC RADIUS для VSA, выберите **Yes. Это**

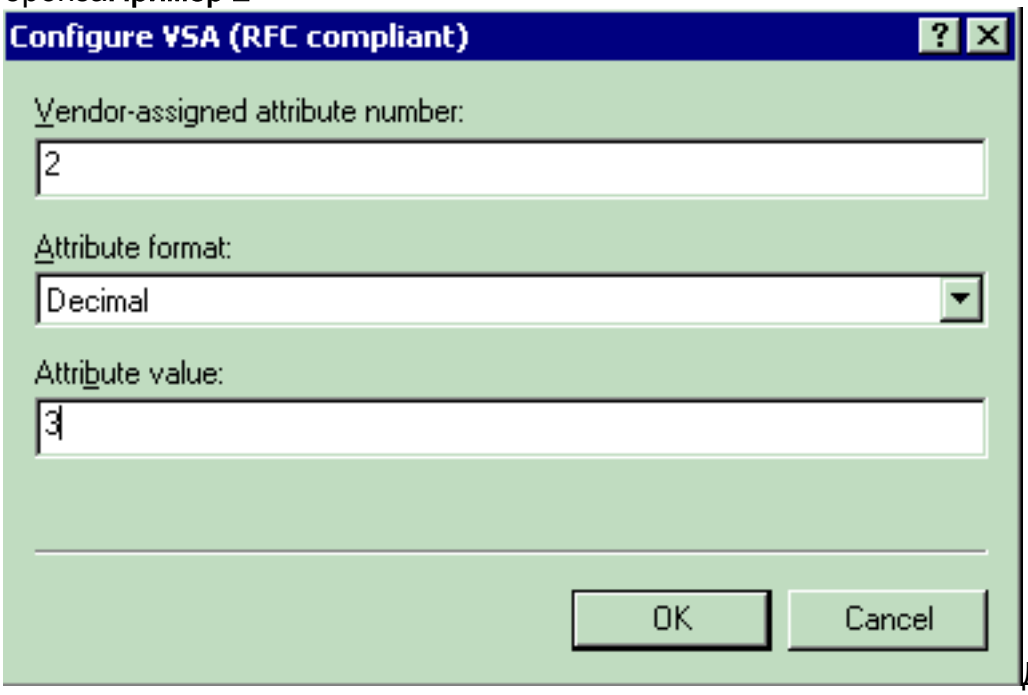


соответствует.. Наж мите **Configure Attribute**.В Настраивать VSA (RFC-совместимый) окно введите

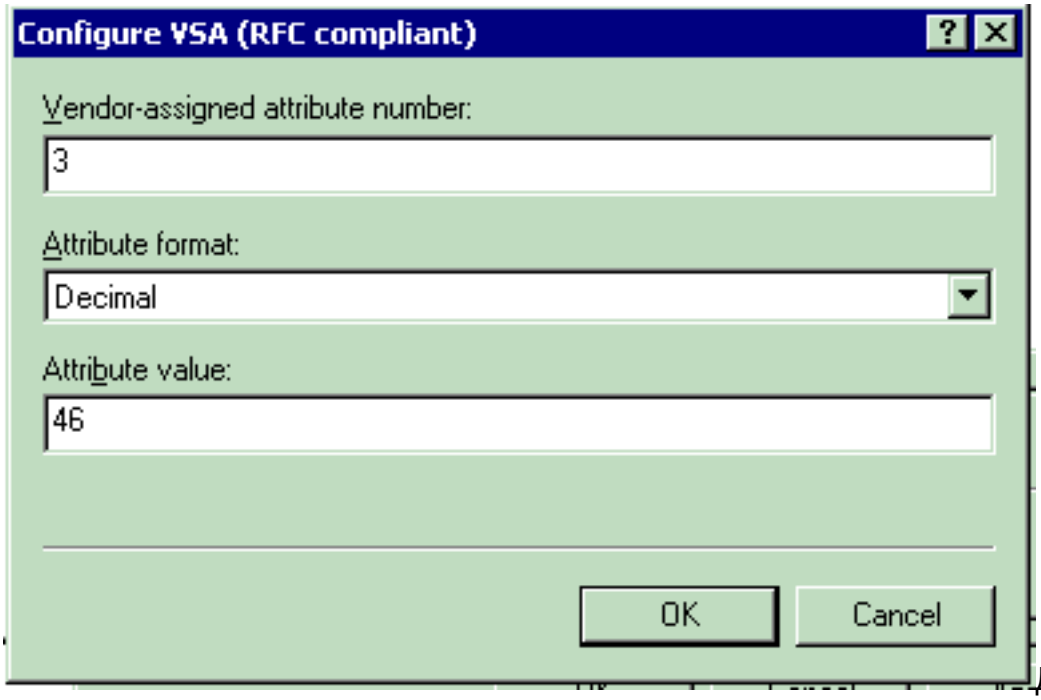
назначенный Поставщиками номер атрибута, Формат атрибута и Значение атрибута, которые зависят от VSA, который вы хотите использовать.Для установки ИДЕНТИФИКАТОРА WLAN на основе для каждого пользователя:**Название атрибута** — ИДЕНТИФИКАТОР WLAN AIRESPACE**Назначенный поставщиками номер атрибута** — 1**Формат атрибута** — целое число/Десятичное число**Значение** — ИДЕНТИФИКАТОР WLAN**Пример 1**



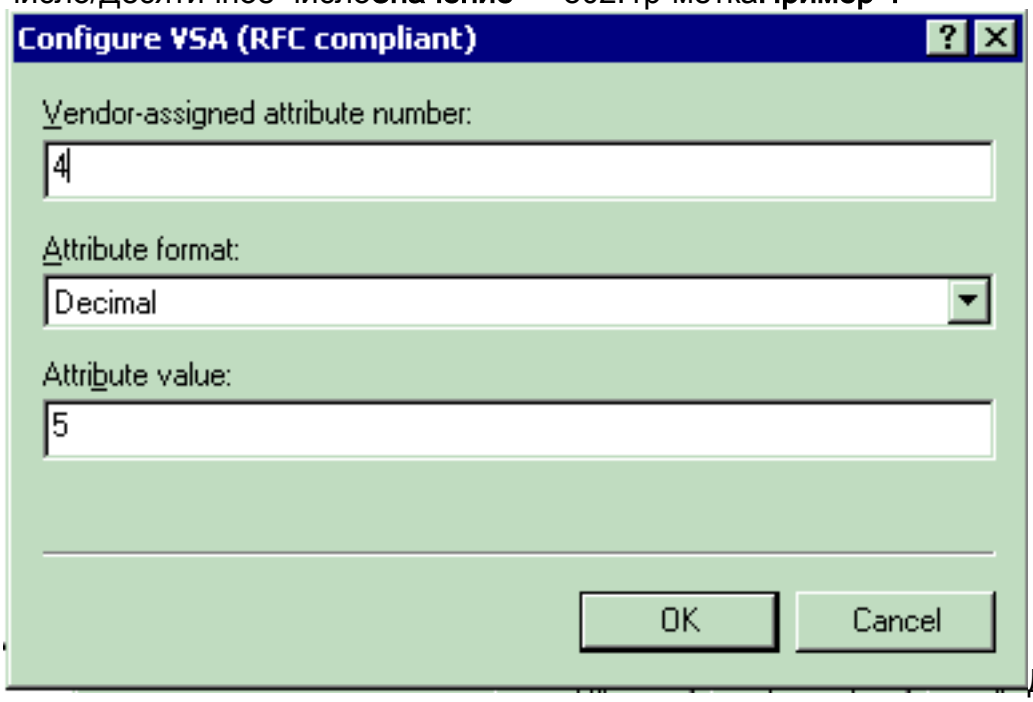
Для установки QoS представляют на основе для каждого пользователя:**Название атрибута** — уровень QoS Airespace**Назначенный поставщиками номер атрибута** — 2**Формат атрибута** — целое число/Десятичное число**Значение** — 0 - серебро; 1 - золото; 2 - платина; 3 - бронза**Пример 2**



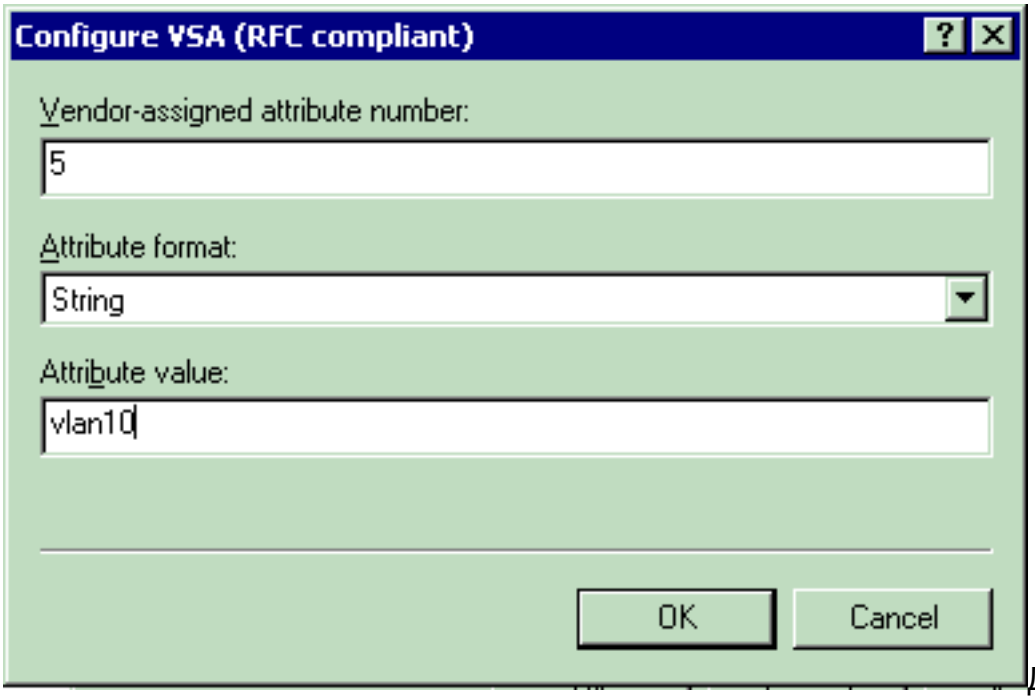
Для установки DSCP-значения на основе для каждого пользователя:**Название атрибута** — DSCP Airespace**Назначенный поставщиками атрибут aumber** — 3**Формат атрибута** — целое число/Десятичное число**Значение** — DSCP-значение**Пример 3**



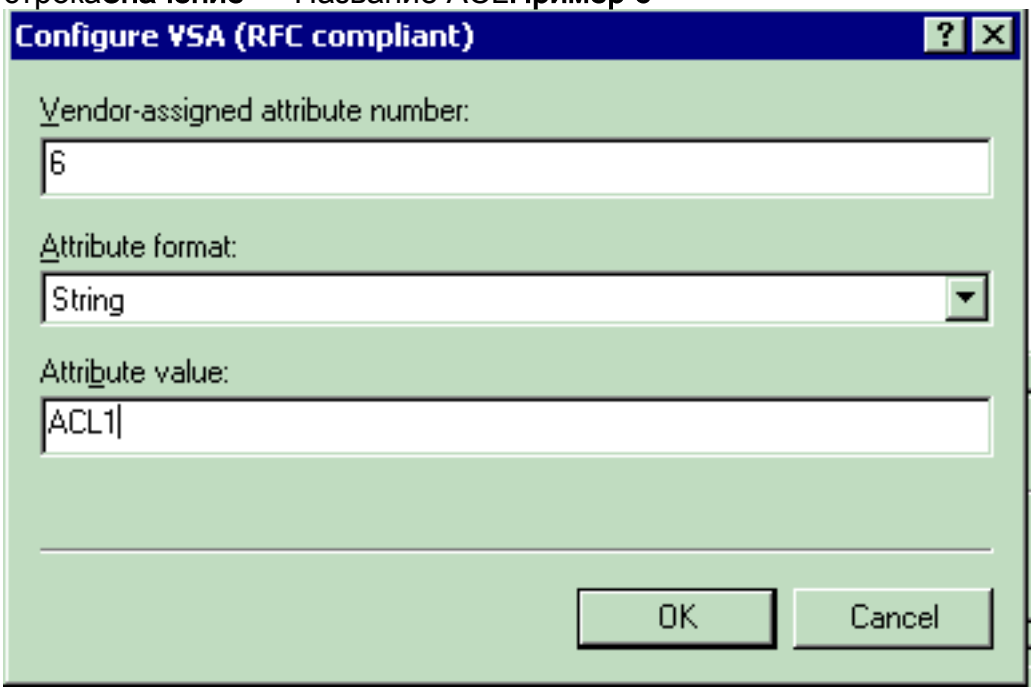
Для установки 802.1p-метки на основе для каждого пользователя:**Название атрибута** — Airespace-802.1p-Tag**Назначенный поставщиками номер атрибута** — 4**Формат атрибута** — целое число/Десятичное число**Значение** — 802.1p-метка**Пример 4**



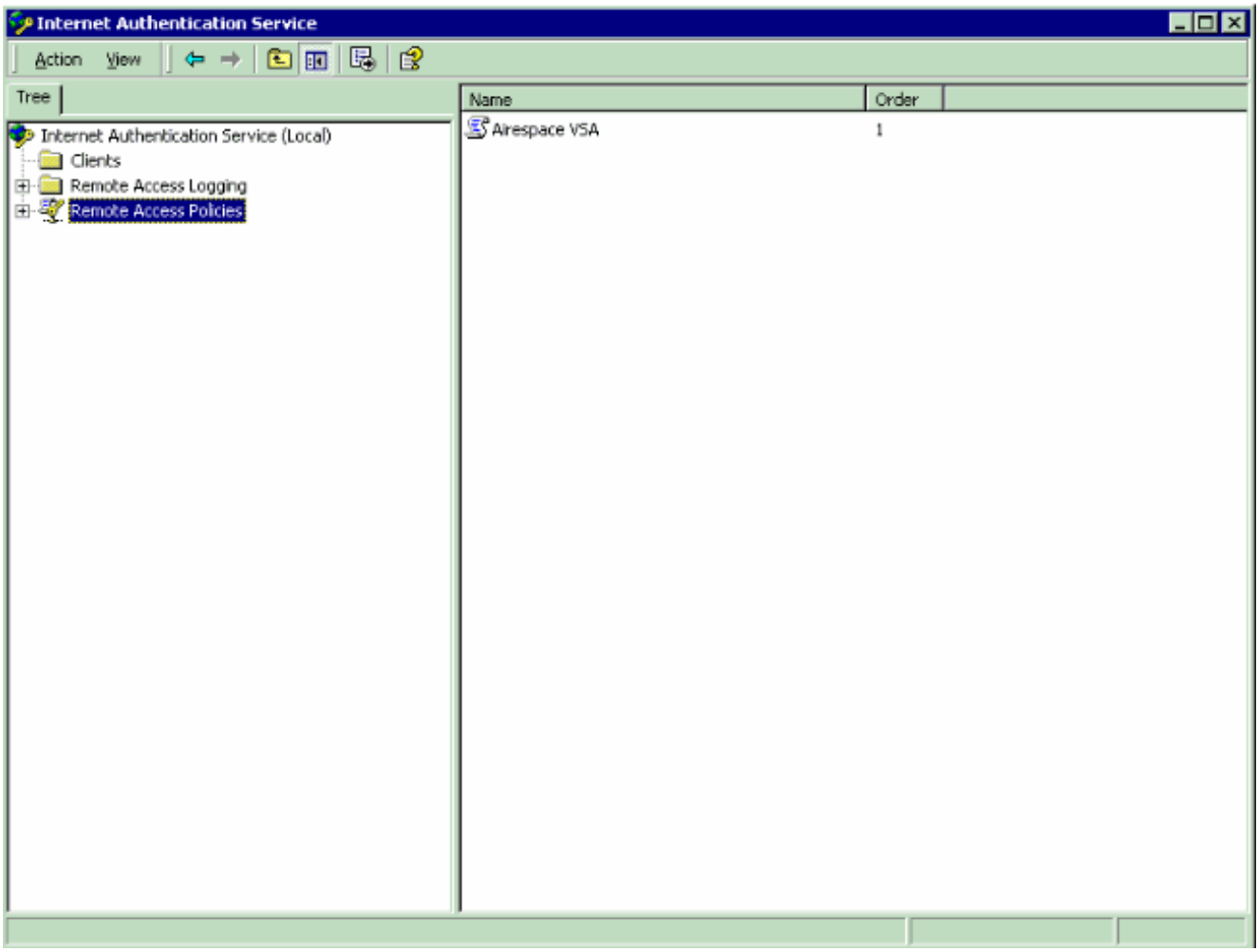
Для установки Interface (VLAN) на основе для каждого пользователя:**Название атрибута** — interface-name Airespace**Назначенный поставщиками номер атрибута** — 5**Формат атрибута** — строка**Значение** — Interface-Name**Пример 5**



Для установки ACL на основе для каждого пользователя:**Название атрибута** — НАЗВАНИЕ ACL AIRESPACE**Назначенный поставщиками номер атрибута** — 6**Формат атрибута** — строка**Значение** — Название ACL**Пример 6**

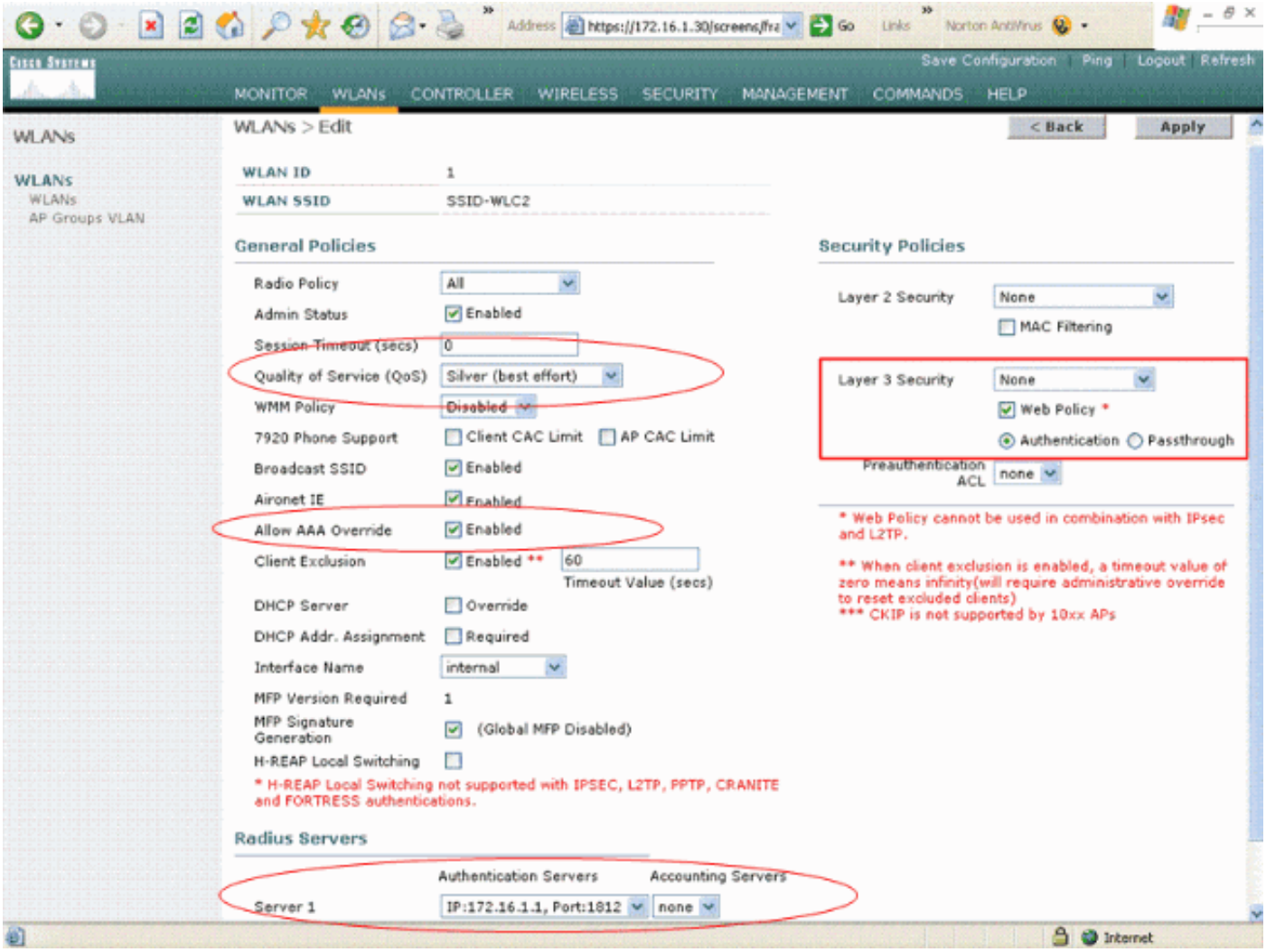


8. Как только вы настроили VSA, нажмите **OK**, пока вы не видите окно Профиля пользователя.
9. Затем нажмите **Finish** для завершения конфигурации.Вы видите новую политику под Политикой Удаленного
доступа.



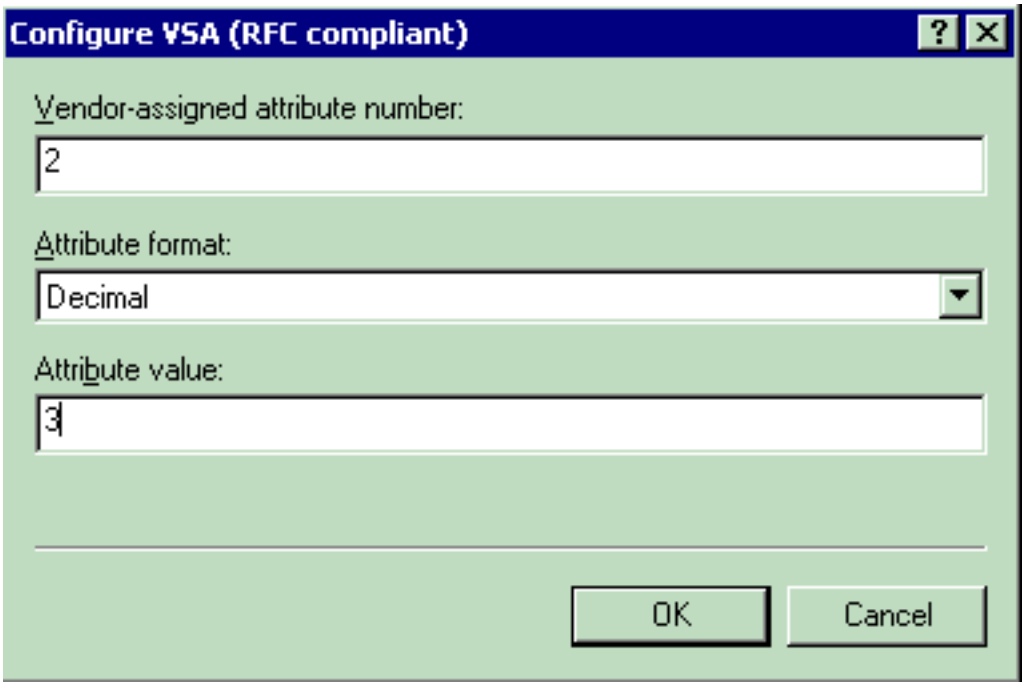
Пример конфигурации

В данном примере WLAN настроен для web-аутентификации. Пользователи аутентифицируются сервером RADIUS IAS, и сервер RADIUS настроен для выделения политик QoS на основе для каждого пользователя.



Как вы можете видеть из этого окна, web-аутентификация включена, сервер проверки подлинности 172.16.1.1, и замена AAA также включена на WLAN. Значение QoS по умолчанию для этого WLAN установлено в Серебро.

На сервере RADIUS IAS настроена Политика Удаленного доступа, который возвращается, Бронза атрибута QoS в RADIUS принимают запрос. Это сделано при настройке VSA, определенного для атрибута QoS.



Посмотрите Настраивание Политики Удаленного доступа по разделу IAS этого документа для получения дальнейшей информации о том, как настроить Политику Удаленного доступа по серверу IAS.

Однажды сервер IAS, WLC и LAP настроены для этой настройки, беспроводные клиенты могут использовать web-аутентификацию для соединения.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Когда пользователь соединяется с WLAN с идентификатором пользователя и паролем, WLC передает учетные данные к серверу RADIUS IAS, который аутентифицирует пользователя против условий и профиля пользователя, настроенного в Политике Удаленного доступа. Если проверка подлинности пользователя успешна, сервер RADIUS возвращается, RADIUS принимают запрос, который также содержит значения замены AAA. В этом случае политика QoS пользователя возвращена.

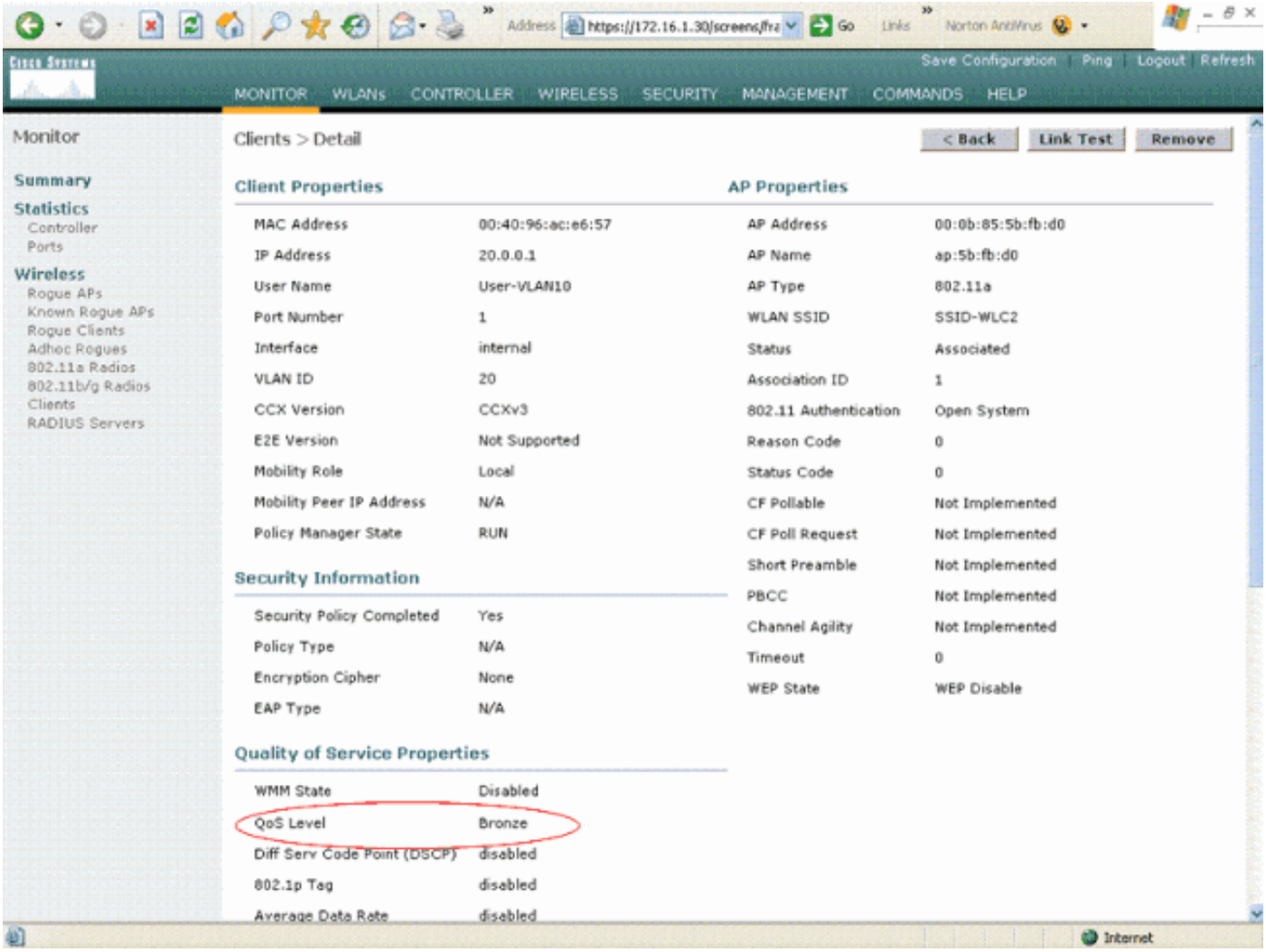
Можно выполнить **команду debug aaa all enable** для наблюдения последовательности событий, которая происходит во время аутентификации. Ниже приведен пример выходных данных:

```
(Cisco Controller) > debug aaa all enable Wed Apr 18 18:14:24 2007: User admin authenticated Wed
Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile
28:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c Wed Apr 18
18:14:24 2007: structureSize.............................70 Wed Apr 18 18:14:24 2007:
resultCode.................................0 Wed Apr 18 18:14:24 2007:
protocolUsed.............................0x00000008 Wed Apr 18 18:14:24 2007:
proxyState................................. 28:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007:
Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-
Type.......................... 0x00000006 (6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02]
Airespace / WLAN-Identifier.............. 0x00000000 (0) (4 bytes) Wed Apr 18 18:14:24 2007:
User admin authenticated Wed Apr 18 18:14:24 2007: 29:1f:00:00:00:00 Returning AAA Error
'Success' (0) for mobile 29:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse:
0xbadff97c Wed Apr 18 18:14:24 2007: structureSize.............................70 Wed Apr 18
18:14:24 2007: resultCode.................................0 Wed Apr 18 18:14:24 2007:
```

```
protocolUsed.................................0x00000008 Wed Apr 18 18:14:24 2007:
proxyState..................................... 29:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007:
Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-
Type............................ 0x00000006 (6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02]
Airespace / WLAN-Identifier.............. 0x00000000 (0) (4 bytes) Wed Apr 18 18:15:08 2007:
Unable to find requested user entry for User-VLAN10 Wed Apr 18 18:15:08 2007:
AuthenticationRequest: 0xa64c8bc Wed Apr 18 18:15:08 2007:
Callback.....................................0x8250c40 Wed Apr 18 18:15:08 2007:
protocolType.................................0x00000001 Wed Apr 18 18:15:08 2007:
proxyState..................................... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007:
Packet contains 8 AVPs (not shown) Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful
transmission of Authentication Packet (id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-
96:ac Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00 00 00 00 00 00 00 00 00
...h............ Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73 65 72 2d 56 4c 41
4e 31 ......User-VLAN1 Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a ba 57 38 11
bc 9a 5d 59 0...2W.*.W8...]Y Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00 01 04
06 ac 10 01 1e 20 ..#............. Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00
00 37 63 01 06 00 00 00 .WLC2....7c..... Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e
30 2e 30 2e 31 1e 0d 31 37 32 ...20.0.0.1..172 Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e
31 2e 33 30 .16.1.30 Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc e4 ea 41 3e 28
7e cc bc ...F?.....A>(~.. Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00 37 63 02
06 00 00 00 03 ..a.....7c...... Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20 37
d0 03 e6 00 00 01 37 ........7......7 Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01
c7 7a 8b 35 20 31 80 00 00 ........z.5.1... Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 00
1b ...... Wed Apr 18 18:15:08 2007: ****Enter processIncomingMessages: response code=2 Wed Apr
18 18:15:08 2007: ****Enter processRadiusResponse: response code=2 Wed Apr 18 18:15:08 2007:
00:40:96:ac:e6:57 Access-Accept received from RADIUS server 172.16.1.1 for mobile
00:40:96:ac:e6:57 receiveId = 0 Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520 Wed
Apr 18 18:15:08 2007: structureSize.............................114 Wed Apr 18 18:15:08 2007:
resultCode.....................................0 Wed Apr 18 18:15:08 2007:
protocolUsed.................................0x00000001 Wed Apr 18 18:15:08 2007:
proxyState..................................... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007:
Packet contains 3 AVPs: Wed Apr 18 18:15:08 2007: AVP[01] Airespace / QOS-
Level..................... 0x00000003 (3) (4 bytes) Wed Apr 18 18:15:08 2007: AVP[02] Service-
Type............................ 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:08 2007: AVP[03]
Class..................................... DATA (30 bytes) Wed Apr 18 18:15:08 2007:
00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Wed Apr 18 18:15:08
2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48, valid bits:
0x3 qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1,
rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: ' Wed Apr 18 18:15:12 2007:
AccountingMessage Accounting Start: 0xa64c8bc Wed Apr 18 18:15:12 2007: Packet contains 13 AVPs:
Wed Apr 18 18:15:12 2007: AVP[01] User-Name.............................. User-VLAN10 (11
bytes) Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port................................ 0x00000001
(1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[03] Nas-Ip-Address.........................
0xac10011e (-1408237282) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[04] NAS-
Identifier........................... 0x574c4332 (1464615730) (4 bytes) Wed Apr 18 18:15:12
2007: AVP[05] Airespace / WLAN-Identifier.............. 0x00000001 (1) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[06] Acct-Session-Id.......................... 4626602c/00:40:96:ac:e6:57/16
(29 bytes) Wed Apr 18 18:15:12 2007: AVP[07] Acct-Authentic.........................
0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[08] Tunnel-
Type............................ 0x0000000d (13) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[09]
Tunnel-Medium-Type...................... 0x00000006 (6) (4 bytes) Wed Apr 18 18:15:12 2007:
AVP[10] Tunnel-Group-Id......................... 0x3230 (12848) (2 bytes) Wed Apr 18 18:15:12
2007: AVP[11] Acct-Status-Type....................... 0x00000001 (1) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[12] Calling-Station-Id...................... 20.0.0.1 (8 bytes) Wed Apr 18
18:15:12 2007: AVP[13] Called-Station-Id...................... 172.16.1.30 (11 bytes)
```

Как вы можете видеть от выходных данных, пользователь аутентифицируется. Затем значения замены AAA возвращены с RADIUS, принимают сообщение. В этом случае пользователю дают политику QoS Бронзы.

Можно проверить это на GUI WLC также. Например:



Примечание: Профиль QoS по умолчанию для этого SSID является Серебряным. Однако, потому что замена AAA выбрана, и пользователь настроен с профилем QoS Бронзы на сервере IAS, профиль QoS по умолчанию отвергнут.

Устранение неполадок

Можно использовать **команду debug aaa all enable** на WLC для устранения проблем конфигурации. Пример выходных данных этой отладки в рабочей сети показывают в Сверять разделе этого документа.

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

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Пример настройки ограничения доступа к WLAN на основе SSID с WLC и Cisco Secure ACS
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация