Отладка аутентификации

Содержание

Введение

В беспроводной связи используются разные способы аутентификации. Наиболее общим типом аутентификации является протокол расширенной аутентификации (EAP) в различных типах и формах. Другие типы аутентификации включают в себя аутентификацию адреса MAC и административную аутентификацию. В данном документе описано, как отлаживать и интерпретировать выходные данные, полученные при отладке аутентификации. Сведения, полученные из этих отладочных данных, являются очень важными при устранении неполадок во время установки беспроводных устройств.

Примечание. Разделы данного документа, которые относятся к продуктам, отличным от продуктов Cisco, основаны на опыте автора, а не на формальном обучении. Они предназначены для удобства работы с описанными процедурами, а не для технической поддержки. Чтобы получить надежную техническую поддержку по продукту, отличному от Cisco, обратитесь в группу технической поддержки по вопросу, касающемуся данного продукта.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с содержанием следующих разделов:

- Аутентификация, связанная с беспроводными сетями
- Интерфейс (CLI) командной строки ПО Cisco IOS®
- Конфигурация сервера RADIUS

Используемые компоненты

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

- Беспроводные продукты, основанные на ПО Cisco IOS любой модели и версии
- Приложение Hilgraeve HyperTerminal

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

Условные обозначения

Подробные сведения о применяемых в документе обозначениях см. в разделе Условные обозначения, используемые в технической документации Cisco.

Сбор отладочных сведений

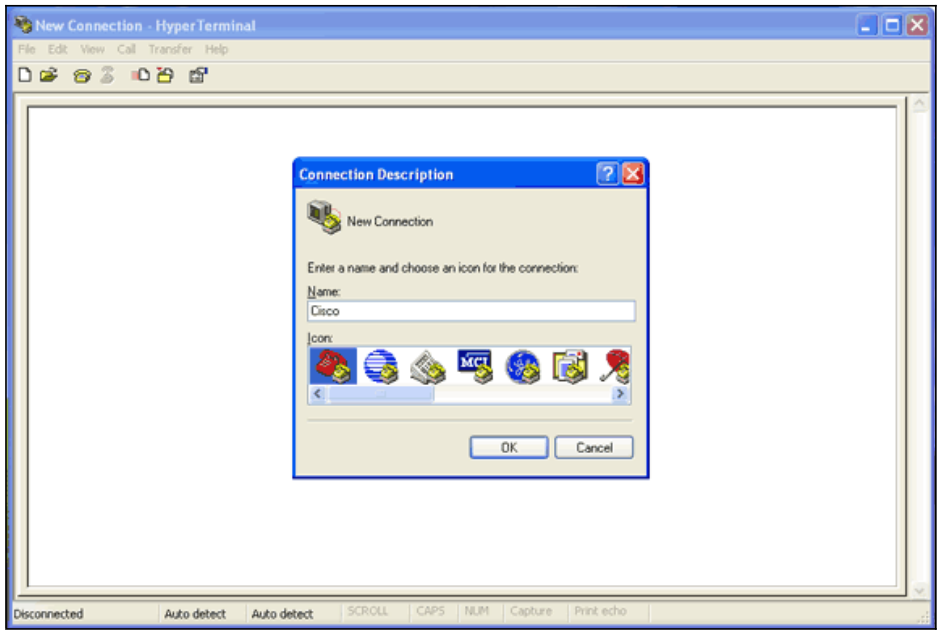
Если не удалось собрать и проанализировать отладочные сведения, они бесполезны. Самый легкий способ собрать эти данные – с помощью функции экранного снимка, встроенной в Telnet или в приложение связи.

В данном примере описывается, как собрать выходные данные с помощью приложения Hilgraeve HyperTerminal . Большинство операционных систем Microsoft Windows содержит программу HyperTerminal, но данную концепцию можно применить к любому приложению эмуляции терминала. Подробные сведения о данном приложении см. в разделе Hilgraeve .

Выполните следующие действия, чтобы настроить HyperTerminal для взаимодействия с точкой доступа (AP) или мостом:

1. Чтобы открыть HyperTerminal, выберите **Start > Programs > System Tools > Communications > HyperTerminal**.

   Рис. 1. Загрузка HyperTerminal



2. После открытия HyperTerminal выполните следующие действия:

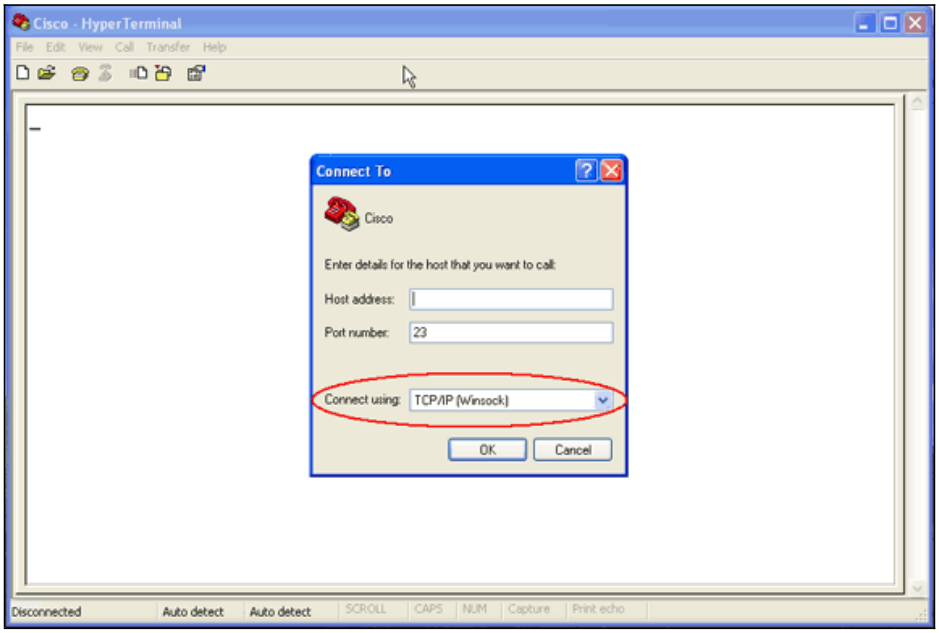
   1. Введите имя соединения.
   2. Выберите значок.
   3. Нажмите **OK**.

3. Для подключения к Telnet выполните следующие действия:

   1. В раскрывающемся меню "Connect Using" выберите **TCP/IP**.
   2. Введите IP-адрес устройства, где необходимо запустить процедуру отладки.

3. Нажмите **OK**.

Рис.2. Подключение к Telnet



4. Выполните следующие действия для подключения к консоли:

1. В раскрывающемся меню "Connect Using" выберите COM-порт, где подключен кабель консоли.
2. Нажмите **OK**.

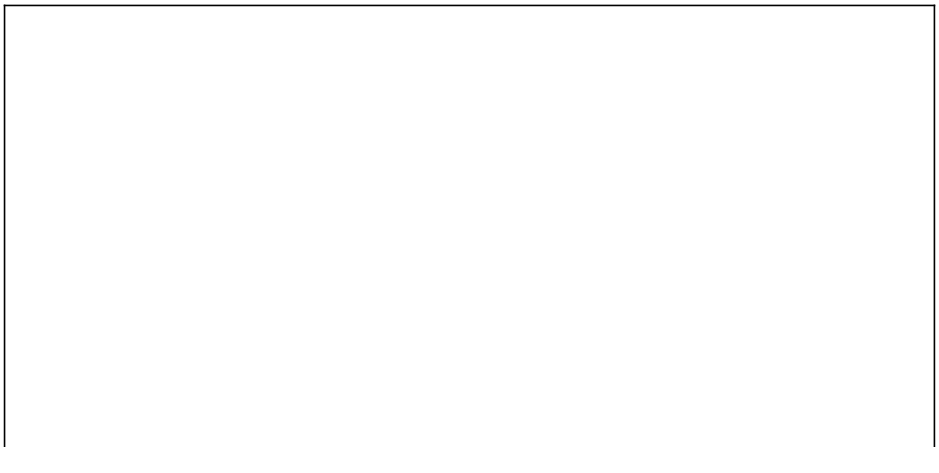
   Отобразится таблица свойств подключения.
3. Установите скорость подключения для порта консоли.
4. Чтобы восстановить настройки порта по умолчанию, нажмите **Restore Defaults**.

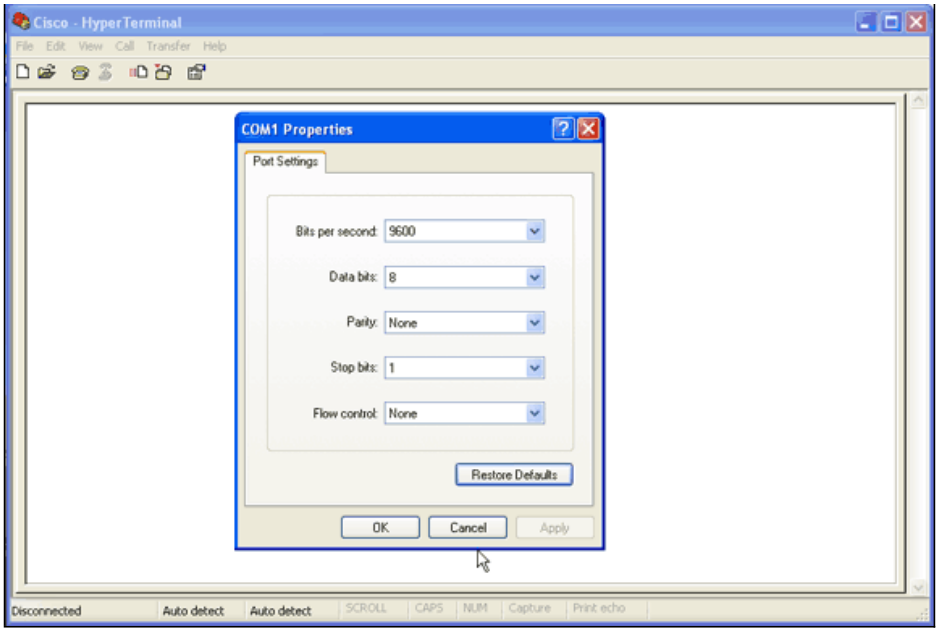
   Примечание. Большинство продуктов Cisco поддерживают настройки порта по умолчанию.

   Настройки порта по умолчанию выглядят следующим образом:

   - Bits per second — 9600
   - Data bits — 8
   - Parity — None
   - Stop bits — 1
   - Flow control — None

Рис. 3. Загрузка COM1





На этом этапе устанавливается соединение Telnet или консольное соединение, и выводится приглашение ввести имя и пароль пользователя.

Примечание. Оборудование Cisco Aironet назначает имя пользователя и пароль *Cisco* по умолчанию (с учетом регистра).

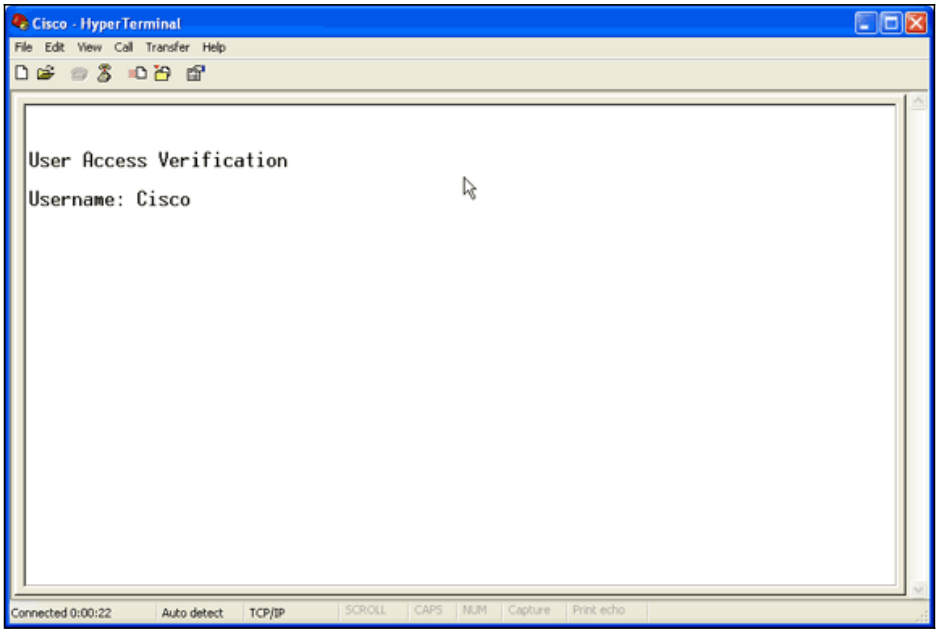
5. Чтобы запустить процедуру отладки, выполните следующие действия:

    1. Выполните команду **enable**, чтобы установить привилегированный режим.
    2. Введите пароль для команды enable.

    Примечание. Необходимо помнить, что пароль по умолчанию для оборудования Aironet – *Cisco* (с учетом регистра).

    Примечание. Чтобы просмотреть выходные данные отладки во время сеанса Telnet, используйте команду **terminal monitor** или **term mon**, чтобы включить монитор терминала.

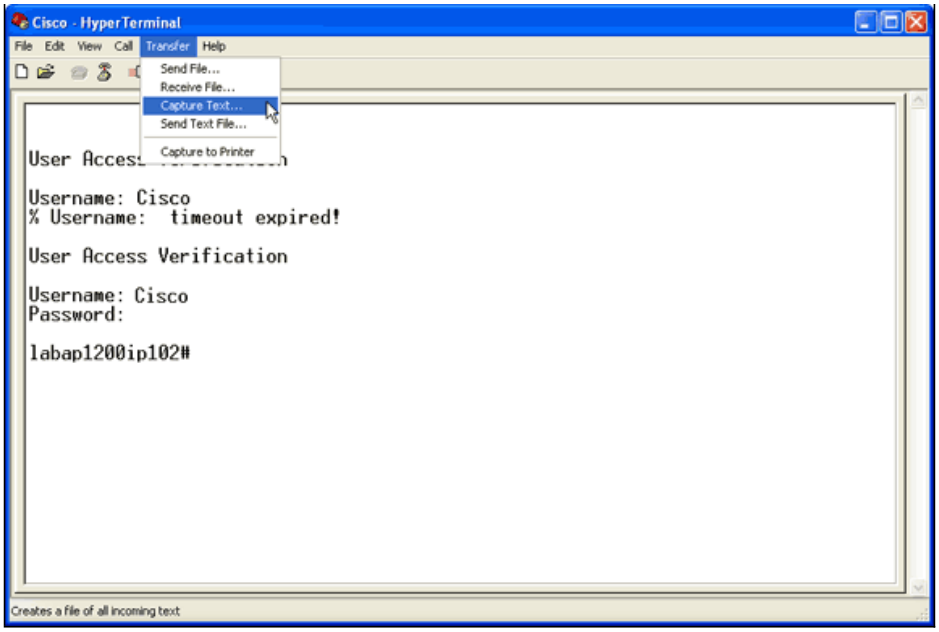
    Рис. 4. Сеанс подключения к Telnet



6. После установки соединения выполните следующие действия, чтобы получить снимок экрана:

    1. В меню Transfer выберите **Capture Text**.

    Рис. 5. Сохранение снимка экрана

1. 

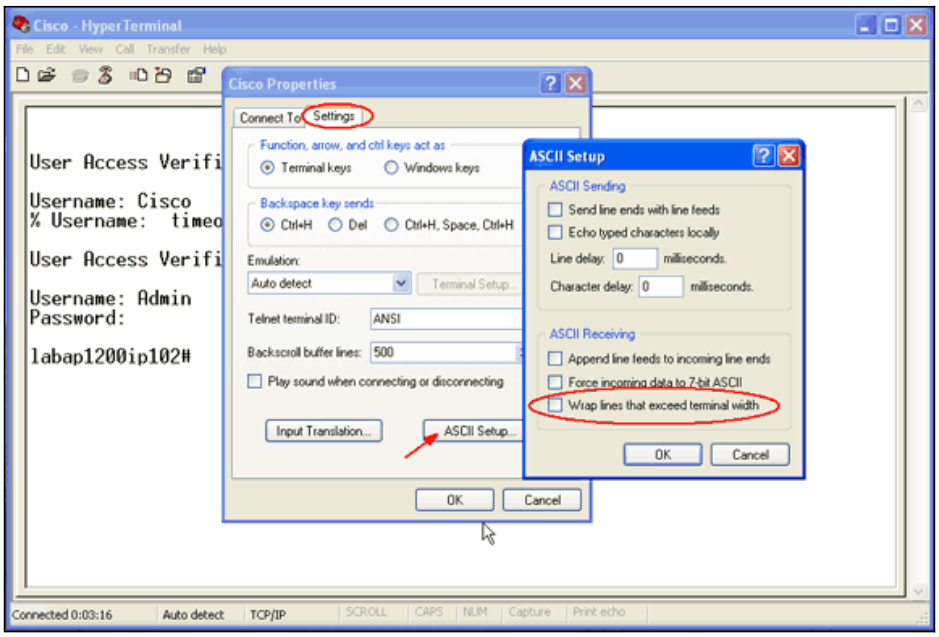
2. Откроется диалоговое окно, в котором будет предложено ввести имя файла выходных данных; введите имя файла.

7. Чтобы отключить свертку экрана, выполните следующие действия.

Примечание. Отключение свертки экрана облегчает чтение отладочных данных.

1. В меню HyperTerminal выберите **File**.
2. Выберите **Properties**.
3. В таблице свойств соединения выберите вкладку **Settings**.
4. Щелкните **ASCII Setup**.
5. Снимите флажок **Wrap lines that exceed terminal width**.
6. Чтобы закрыть окно ASCII Settings, нажмите **OK**.
7. Нажмите **OK**, чтобы закрыть страницу свойств соединения.

Рис. 6. Загрузка ASCII



Теперь, когда можно ввести выходные данные экрана в текстовый файл, процедуры отладки выполняются в зависимости от согласования. В следующих разделах описывается тип согласованного соединения, обеспечиваемый процедурами отладки.

Протокол расширенной аутентификации (EAP)

Следующие процедуры отладки являются полезными для аутентификации EAP:

- **debug radius authentication** – выходные данные этой команды отладки начинаются со слова: `RADIUS`.
- **debug dot11 aaa authenticator process** – выходные данные этой команды отладки начинаются с текста: `dot11_auth_dot1x_`.
- **debug dot11 aaa authenticator state-machine** – выходные данные этой команды отладки начинаются с текста: `dot11_auth_dot1x_run_rfsm`.

Представленные ниже отладочные данные содержат:

- Данные, выводимые во фрагментах взаимодействия с RADIUS, диалога аутентификации
- Выполняемые действия в диалоге аутентификации
- Различные состояния, через которые проходит диалог аутентификации

В данном примере показана успешная аутентификация протокола LEAP (Облегченный протокол расширенной аутентификации).

Пример успешной аутентификации EAP

```
Apr  8 17:45:48.208: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Apr  8 17:45:48.208: dot11_auth_dot1x_send_id_req_to_client:
  sending identity request for 0002.8aa6.304f
Apr  8 17:45:48.208: dot11_auth_dot1x_send_id_req_to_client:
  Started timer client_timeout 30 seconds
Apr  8 17:45:48.210: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,EAP_START) for 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:
   sending identity request for 0002.8aa6.304f
Apr  8 17:45:48.210: dot11_auth_dot1x_send_id_req_to_client:
   Started timer client_timeout 30 seconds
Apr  8 17:45:48.212: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.212: dot11_auth_parse_client_pak:
   id is not matching req-id:1resp-id:2, waiting for response
Apr  8 17:45:48.213: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.213: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0002.8aa6.304f
Apr  8 17:45:48.214: dot11_auth_dot1x_send_response_to_server:
   Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.214: dot11_auth_dot1x_send_response_to_server:
   tarted timer server_timeout 60 seconds
Apr  8 17:45:48.214: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.214: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
   [labap1200ip1]
Apr  8 17:45:48.215: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.215: RADIUS(0000001C): Storing nasport 17 in rad_db
Apr  8 17:45:48.215: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.215: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.216: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.216: RADIUS(0000001C): sending
Apr  8 17:45:48.216: RADIUS(0000001C): Send Access-Request
   to 10.0.0.3:1645 id 21645/93, len 139
Apr  8 17:45:48.216: RADIUS:  authenticator 92 26 A8 31 ED 60 6A 88
   - 84 8C 80 B2 B8 26 4C 04
Apr  8 17:45:48.216: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.216: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.217: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.217: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.217: RADIUS:  Service-Type        [6]   6   Login  [1]
```

```
Apr  8 17:45:48.217: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.217: RADIUS:  EAP-Message         [79]  14
Apr  8 17:45:48.218: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
   [?????aironet]
Apr  8 17:45:48.218: RADIUS:  NAS-Port-Type       [61]  6   802.11
   wireless     [19]
Apr  8 17:45:48.218: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.218: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.218: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.224: RADIUS: Received from id 21645/93 10.0.0.3:1645,
   Access-Challenge, len 69
Apr  8 17:45:48.224: RADIUS:  authenticator C8 6D 9B B3 67 60 44 29
   - CC AB 39 DE 00 A9 A8 CA
Apr  8 17:45:48.224: RADIUS:  EAP-Message         [79]  25
Apr  8 17:45:48.224: RADIUS:   01 43 00 17 11 01 00 08 63 BB E7 8C 0F AC EB 9A
   [?C??????c???????]
Apr  8 17:45:48.225: RADIUS:   61 69 72 6F 6E 65 74
   [aironet]
Apr  8 17:45:48.225: RADIUS:  Session-Timeout     [27]  6   20
Apr  8 17:45:48.225: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.226: RADIUS(0000001C): Received from id 21645/93
Apr  8 17:45:48.226: RADIUS/DECODE: EAP-Message fragments, 23, total 23 bytes
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: GET_CHALLENGE_RESPONSE
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp: found eap pak in
   server response
Apr  8 17:45:48.226: dot11_auth_dot1x_parse_aaa_resp: found session timeout
   20 sec
Apr  8 17:45:48.227: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_REPLY) for
   0002.8aa6.304f
Apr  8 17:45:48.227: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.227: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 20 seconds
Apr  8 17:45:48.232: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.232: dot11_auth_dot1x_run_rfsm: Executing Action
   (CLIENT_WAIT,CLIENT_REPLY) for 0002.8aa6.304f
Apr  8 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
   Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.232: dot11_auth_dot1x_send_response_to_server:
   Started timer server_timeout 60 seconds
Apr  8 17:45:48.233: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.234: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
   [labap1200ip1]
Apr  8 17:45:48.234: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.234: RADIUS(0000001C): Using existing nas_port 17
Apr  8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.234: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.234: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.234: RADIUS(0000001C): sending
Apr  8 17:45:48.234: RADIUS(0000001C): Send Access-Request to
   10.0.0.3:1645 id 21645/94, len 166
Apr  8 17:45:48.235: RADIUS:  authenticator 93 B5 CC B6 41 97 A0 85
   - 1B 4D 13 0F 6A EE D4 11
Apr  8 17:45:48.235: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.235: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.236: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.236: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.236: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 17:45:48.236: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.236: RADIUS:  EAP-Message         [79]  41
Apr  8 17:45:48.236: RADIUS:   02 43 00 27 11 01 00 18 30 9F 55 AF 05 03 71 7D
   [?C?'????0?U???q}]
Apr  8 17:45:48.236: RADIUS:   25 41 1B B0 F4 A9 7C EE F5 51 24 9A FC 6D 51 6D
   [?A????|??Q$??mQm]
Apr  8 17:45:48.237: RADIUS:   61 69 72 6F 6E 65 74                  [aironet]
Apr  8 17:45:48.237: RADIUS:  NAS-Port-Type       [61]  6   802.11
   wireless   [19]
Apr  8 17:45:48.237: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.238: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.238: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.242: RADIUS: Received from id 21645/94 10.0.0.3:1645,
   Access-Challenge, len 50
Apr  8 17:45:48.243: RADIUS:  authenticator 59 2D EE 24 CF B2 87 AF
   - 86 D0 C9 00 79 BE 6E 1E
Apr  8 17:45:48.243: RADIUS:  EAP-Message         [79]  6
Apr  8 17:45:48.243: RADIUS:   03 43 00 04
   [?C??]
Apr  8 17:45:48.244: RADIUS:  Session-Timeout     [27]  6   20
Apr  8 17:45:48.244: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.244: RADIUS(0000001C): Received from id 21645/94
```

```
Apr  8 17:45:48.244: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:45:48.244: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: GET_CHALLENGE_RESPONSE
Apr  8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp:
   found eap pak in server response
Apr  8 17:45:48.245: dot11_auth_dot1x_parse_aaa_resp:
   found session timeout 20 sec
Apr  8 17:45:48.245: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_REPLY)
for 0002.8aa6.304f
Apr  8 17:45:48.245: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.246: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 20 seconds
Apr  8 17:45:48.249: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 17:45:48.250: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0002.8aa6.304f
Apr  8 17:45:48.250: dot11_auth_dot1x_send_response_to_server:
   Sending client 0002.8aa6.304f data to server
Apr  8 17:45:48.250: dot11_auth_dot1x_send_response_to_server:
   Started timer server_timeout 60 seconds
Apr  8 17:45:48.250: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:45:48.251: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
   [labap1200ip1]
Apr  8 17:45:48.251: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:45:48.251: RADIUS(0000001C): Using existing nas_port 17
Apr  8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.252: RADIUS/ENCODE(0000001C): acct_session_id: 28
Apr  8 17:45:48.252: RADIUS(0000001C): Config NAS IP: 10.0.0.102
Apr  8 17:45:48.252: RADIUS(0000001C): sending
Apr  8 17:45:48.252: RADIUS(0000001C): Send Access-Request to
   10.0.0.3:1645 id 21645/95, len 150
Apr  8 17:45:48.252: RADIUS:  authenticator 39 1C A5 EF 86 9E BA D1
   - 50 FD 58 80 A8 8A BC 2A
Apr  8 17:45:48.253: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 17:45:48.253: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:45:48.253: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:45:48.253: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:45:48.254: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 17:45:48.254: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.254: RADIUS:  EAP-Message         [79]  25
Apr  8 17:45:48.254: RADIUS:   01 43 00 17 11 01 00 08 50 9A 67 2E 7D 26 75 AA
   [?C??????P?g.}&u?]
Apr  8 17:45:48.254: RADIUS:   61 69 72 6F 6E 65 74
   [aironet]
Apr  8 17:45:48.254: RADIUS:  NAS-Port-Type       [61]  6   802.11
   wireless  [19]
Apr  8 17:45:48.254: RADIUS:  NAS-Port            [5]   6   17
Apr  8 17:45:48.255: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:45:48.255: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 17:45:48.260: RADIUS: Received from id 21645/95 10.0.0.3:1645,
   Access-Accept, len 206
Apr  8 17:45:48.260: RADIUS:  authenticator 39 13 3C ED FC 02 68 63
   - 24 13 1B 46 CF 93 B8 E3
Apr  8 17:45:48.260: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr  8 17:45:48.261: RADIUS:  EAP-Message         [79]  41
Apr  8 17:45:48.261: RADIUS:   02 00 00 27 11 01 00 18 FA 53 D0 29 6C 9D 66 8E
   [???'?????S?)l?f?]
Apr  8 17:45:48.262: RADIUS:   C4 A3 CD 54 08 8C 35 7C 74 0C 6A EF D4 6D 30 A4
   [???T??5|t?j??m0?]
Apr  8 17:45:48.262: RADIUS:   61 69 72 6F 6E 65 74                  [aironet]
Apr  8 17:45:48.262: RADIUS:  Vendor, Cisco       [26]  59
Apr  8 17:45:48.262: RADIUS:   Cisco AVpair       [1]   53
   "leap:session-key=G:3asil;mwerAEJNYH-JxI,"
Apr  8 17:45:48.262: RADIUS:  Vendor, Cisco       [26]  31
Apr  8 17:45:48.262: RADIUS:   Cisco AVpair       [1]   25
   "auth-algo-type=eap-leap"
Apr  8 17:45:48.262: RADIUS:  Class               [25]  31
Apr  8 17:45:48.263: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 31 64 36
   [CISCOACS:00001d6]
Apr  8 17:45:48.263: RADIUS:   33 2F 30 61 30 30 30 30 36 36 2F 31 37
   [3/0a000066/17]
Apr  8 17:45:48.263: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:45:48.264: RADIUS(0000001C): Received from id 21645/95
Apr  8 17:45:48.264: RADIUS/DECODE: EAP-Message fragments, 39, total 39 bytes
Apr  8 17:45:48.264: found leap session key
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: PASS
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
   found eap pak in server response
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
   found leap session key in server response
```

```
Apr  8 17:45:48.265: dot11_auth_dot1x_parse_aaa_resp:
   leap session key length 16
Apr  8 17:45:48.266: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_PASS) for 0002.8aa6.304f
Apr  8 17:45:48.266: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0002.8aa6.304f
Apr  8 17:45:48.266: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 20 seconds
Apr  8 17:45:48.266: %DOT11-6-ASSOC: Interface Dot11Radio0,
   Station RKIBBE-W2K4 0002.8aa6.304f Associated KEY_MGMT[NONE]
```

Обратите внимание на поток сообщений в отладочных данных **state-machine**. Происходит последовательное прохождение через несколько состояний.

1. EAP_START
2. CLIENT_WAIT
3. CLIENT_REPLY
4. SERVER_WAIT
5. SERVER_REPLY

   Примечание. При взаимодействии двух состояний может быть несколько повторов CLIENT_WAIT и CLIENT_REPLY, а также SERVER_WAIT и SERVER_REPLY.
6. SERVER_PASS

Отладочные данные **process** отображают прохождение отдельного шага через каждое состояние. Отладочные данные **radius** отображают фактическое взаимодействие между сервером аутентификации и клиентом. Самый легкий способ работы с процедурами отладки EAP – это наблюдать за последовательностью сообщений о состоянии машин при прохождении каждого состояния.

Если происходит ошибка в согласовании в отладочных данных **state-machine** отображается причина. Примеры сообщений выглядят следующим образом:

- **CLIENT TIMEOUT** – данное состояние означает, что клиент не отправил ответ в течение установленного периода времени. Ошибка при отправке ответа может произойти по следующим причинам:
  - Проблема ПО клиента.
  - Время ожидания ответа клиента EAP (подзакладка "EAP Authentication" под "Advanced Security") истекло.

  Некоторым EAP, в частности защищенному EAP (PEAP), требуется более 30 секунд для завершения аутентификации. Установите таймер на другое значение (от 90 до 120 секунд).

  Это пример попытки CLIENT TIMEOUT:

Пример CLIENT TIMEOUT

```
Apr 12 17:51:09.373: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Apr 12 17:51:09.373: dot11_auth_dot1x_send_id_req_to_client:
   sending identity request for 0040.96a0.3758
Apr 12 17:51:09.374: dot11_auth_dot1x_send_id_req_to_client:
   Started timer client_timeout 30 seconds
Apr 12 17:51:39.358: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,TIMEOUT) for 0040.96a0.3758
Apr 12 17:51:39.358: dot11_auth_dot1x_send_client_fail:
   Authentication failed for 0040.96a0.3758
Apr 12 17:51:39.358: %DOT11-7-AUTH_FAILED:
   Station 0040.96a0.3758 Authentication failed
```

Примечание. Сообщение о системной ошибке может выглядеть следующим образом:

```
%DOT11-4-MAXRETRIES: Packet to client xxxx.xxxx.xxxx reached
   max retries, removing the client
```

Примечание. Эти сообщения об ошибке не обязательно свидетельствуют о проблеме, связанной с радиосвязью (RF).

- **Несоответствие общего секретного ключа между AP и сервером RADIUS** – в данном примере регистрации сервер RADIUS не принимает запрос об аутентификации от AP. AP продолжает отправлять запрос на сервер RADIUS, но RADIUS отклоняет запрос, так как не соответствует общий секретный ключ точки доступа.

  Чтобы устранить данную проблему, убедитесь, что AP и сервер RADIUS используют общий секретный ключ.

Несоответствие общего секретного ключа между AP и сервером RADIUS

```
Jun  2 15:58:13.553: %RADIUS-4-RADIUS_DEAD:
   RADIUS server 10.10.1.172:1645, 1646 is not responding.
Jun  2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server
   10.10.1.172:1645,1646 has returned.
Jun  2 15:58:23.664: %DOT11-7-AUTH_FAILED: Station 0040.96a0.3758
   Authentication failed
```

- **`server_timeout`** – данное состояние означает, что сервер аутентификации не отправил ответ в течение установленного периода времени. Ошибка при отправке ответа может произойти из-за проблемы на сервере. Проверьте наличие следующих ситуаций:

  - У AP есть возможность IP-подключения к серверу аутентификации.

    Примечание. Чтобы проверить возможность подключения, можно пользоваться командой **ping**.

  - Номера портов аутентификации и учета установлены для сервера правильно.

    Примечание. Номера портов можно проверить на вкладке "Server Manager".

  - Служба аутентификации запущена и работает.

  Это пример попытки `server_timeout`:

Пример `server_timeout`

```
Apr  8 20:02:55.469: dot11_auth_dot1x_start:
   in the dot11_auth_dot1x_start
Apr  8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client:
   sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.469: dot11_auth_dot1x_send_id_req_to_client:
   Started timer client_timeout 30 seconds
Apr  8 20:02:55.470: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,EAP_START) for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
   sending identity request for 0002.8aa6.304f
Apr  8 20:02:55.470: dot11_auth_dot1x_send_id_req_to_client:
   Started timer client_timeout 30 seconds
Apr  8 20:02:55.471: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.472: dot11_auth_parse_client_pak:
   id is not matching req-id:1resp-id:2, waiting for response
Apr  8 20:02:55.474: dot11_auth_parse_client_pak:
   Received EAPOL packet from 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0002.8aa6.304f
Apr  8 20:02:55.474: dot11_auth_dot1x_send_response_to_server:
   Sending client 0002.8aa6.304f data to server
Apr  8 20:02:55.475: dot11_auth_dot1x_send_response_to_server:
```

```
   Started timer server_timeout 60 seconds
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [248] 14
Apr  8 20:02:55.476: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
   [labap1200ip1]
Apr  8 20:02:55.476: RADIUS:  AAA Unsupported     [150] 2
Apr  8 20:02:55.476: RADIUS(00000031): Storing nasport 32 in rad_db
Apr  8 20:02:55.476: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.476: RADIUS/ENCODE(00000031): acct_session_id: 49
Apr  8 20:02:55.477: RADIUS(00000031): Config NAS IP: 10.0.0.102
Apr  8 20:02:55.477: RADIUS(00000031): sending
Apr  8 20:02:55.477: RADIUS(00000031): Send Access-Request
   to 10.0.0.3:1234 id 21645/145, len 139
Apr  8 20:02:55.478: RADIUS:  authenticator B6 F7 BB 41 0E 9F 44 D1
   - 9A F8 E2 D7 5D 70 F2 76
Apr  8 20:02:55.478: RADIUS:  User-Name           [1]   9   "aironet"
Apr  8 20:02:55.478: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 20:02:55.478: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 20:02:55.478: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 20:02:55.478: RADIUS:  Service-Type        [6]   6   Login        [1]
Apr  8 20:02:55.478: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 20:02:55.478: RADIUS:  EAP-Message         [79]  14
Apr  8 20:02:55.479: RADIUS:   02 02 00 0C 01 61 69 72 6F 6E 65 74
   [?????aironet]
Apr  8 20:02:55.479: RADIUS:  NAS-Port-Type       [61]  6   802.11
   wireless [19]
Apr  8 20:02:55.479: RADIUS:  NAS-Port            [5]   6   32
Apr  8 20:02:55.479: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 20:02:55.480: RADIUS:  Nas-Identifier      [32]  16  "labap1200ip102"
Apr  8 20:03:00.478: RADIUS:
   Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:05.475: RADIUS:
   Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:10.473: RADIUS:
   Retransmit to (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS:
   No response from (10.0.0.3:1234,1234) for id 21645/145
Apr  8 20:03:15.470: RADIUS/DECODE:
   parse response no app start; FAIL
Apr  8 20:03:15.470: RADIUS/DECODE:
   parse response; FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: FAIL
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
   found eap pak in server response
Apr  8 20:03:15.470: dot11_auth_dot1x_parse_aaa_resp:
   detailed aaa_status 1
Apr  8 20:03:15.471: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_FAIL) for 0002.8aa6.304f
Apr  8 20:03:15.471: dot11_auth_dot1x_send_client_fail:
   Authentication failed for 0002.8aa6.304f
Apr  8 20:03:15.471: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
   Authentication failed
```

- **SERVER_FAIL** – данное состояние означает, что серверу не удалось отправить ответ об аутентификации на основе учетных данных пользователя. Отладочные данные RADIUS, предшествующие данной ошибке, отображают имя пользователя, представленное серверу аутентификации. Проверьте регистрацию неудачных попыток (Failed Attempts) на сервере аутентификации для получения дополнительных сведений о том, почему сервер отказал в доступе клиенту.

  Это пример попытки SERVER_FAIL:

Пример SERVER_FAIL

```
Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
   Sending client 0002.8aa6.304f data to server
Apr  8 17:46:13.604: dot11_auth_dot1x_send_response_to_server:
   Started timer server_timeout 60 seconds
Apr  8 17:46:13.605: RADIUS:  AAA Unsupported     [248] 14
Apr  8 17:46:13.605: RADIUS:   6C 61 62 61 70 31 32 30 30 69 70 31
   [labap1200ip1]
Apr  8 17:46:13.606: RADIUS:  AAA Unsupported     [150] 2
Apr  8 17:46:13.606: RADIUS(0000001D): Using existing nas_port 18
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS/ENCODE(0000001D): acct_session_id: 29
Apr  8 17:46:13.606: RADIUS(0000001D): Config NAS IP: 10.0.0.102
Apr  8 17:46:13.606: RADIUS(0000001D): sending
Apr  8 17:46:13.607: RADIUS(0000001D): Send Access-Request
   to 10.0.0.3:1645 id 21645/97, len 176
```

```
Apr  8 17:46:13.607: RADIUS:  authenticator 88 82 8C BB DC 78 67 76
   - 36 88 1D 89 2B DC C9 99
Apr  8 17:46:13.607: RADIUS:  User-Name           [1]   14  "unknown_user"
Apr  8 17:46:13.607: RADIUS:  Framed-MTU          [12]  6   1400
Apr  8 17:46:13.608: RADIUS:  Called-Station-Id   [30]  16  "0005.9a39.0374"
Apr  8 17:46:13.608: RADIUS:  Calling-Station-Id  [31]  16  "0002.8aa6.304f"
Apr  8 17:46:13.608: RADIUS:  Service-Type        [6]   6   Login   [1]
Apr  8 17:46:13.608: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.608: RADIUS:  EAP-Message         [79]  46
Apr  8 17:46:13.608: RADIUS:  02 44 00 2C 11 01 00 18 02
   69 C3 F1 B5 90 52 F7    [?D?,?????i????R?]
Apr  8 17:46:13.609: RADIUS:
   B2 57 FF F0 74 8A 80 59 31 6D C7 30 D3 D0 AF 65
   [?W??t??Y1m?0???e]
Apr  8 17:46:13.609: RADIUS:   75 6E 6B 6E 6F 77 6E 5F 75 73 65 72
   [unknown_user]
Apr  8 17:46:13.609: RADIUS:  NAS-Port-Type       [61]  6   802.11
   wireless           [19]
Apr  8 17:46:13.609: RADIUS:  NAS-Port            [5]   6   18
Apr  8 17:46:13.610: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr  8 17:46:13.610: RADIUS:  Nas-Identifier      [32]  16
   "labap1200ip102"
Apr  8 17:46:13.622: RADIUS: Received from id 21645/97
   10.0.0.3:1645, Access-Reject, len 56
Apr  8 17:46:13.622: RADIUS:  authenticator 55 E0 51 EF DA CE F7 78
   - 92 72 3D 97 8F C7 97 C3
Apr  8 17:46:13.622: RADIUS:  EAP-Message         [79]  6
Apr  8 17:46:13.623: RADIUS:   04 44 00 04                          [?D??]
Apr  8 17:46:13.623: RADIUS:  Reply-Message       [18]  12
Apr  8 17:46:13.623: RADIUS:   52 65 6A 65 63 74 65 64 0A 0D  [Rejected??]
Apr  8 17:46:13.623: RADIUS:  Message-Authenticato[80]  18  *
Apr  8 17:46:13.624: RADIUS(0000001D): Received from id 21645/97
Apr  8 17:46:13.624: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Apr  8 17:46:13.624: RADIUS/DECODE: Reply-Message fragments,
   10, total 10 bytes
Apr  8 17:46:13.624: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: FAIL
Apr  8 17:46:13.625: dot11_auth_dot1x_parse_aaa_resp:
   found eap pak in server response
Apr  8 17:46:13.625: dot11_auth_dot1x_run_rfsm:
   xecuting Action(SERVER_WAIT,SERVER_FAIL) for 0002.8aa6.304f
Apr  8 17:46:13.625: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0002.8aa6.304f
Apr  8 17:46:13.626: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 20 seconds
Apr  8 17:46:13.626: dot11_auth_dot1x_send_client_fail:
   Authentication failed for 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-6-DISASSOC: Interface Dot11Radio0,
   Deauthenticating Station 0002.8aa6.304f
Apr  8 17:46:13.626: %DOT11-7-AUTH_FAILED: Station 0002.8aa6.304f
   Authentication failed
```

- **No Response from Client** – в данном примере сервер radius передает сообщение на сервер AP, который перенаправляет его соответствующему клиенту. В итоге клиент не отвечает серверу AP. Таким образом, сервер AP разрывает аутентификацию с клиентом после максимального количества повторов.

Отсутствует ответ от клиента

```
Sep 22 08:42:04: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0040.96a0.3758
Sep 22 08:42:04: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 30 seconds
Sep 22 08:42:04: %DOT11-6-ASSOC: Interface Dot11Radio0,
   Station arlit1ad1hd6j91 0040.96a0.3758 Associated KEY_MGMT[NONE]
Sep 22 10:35:10: %DOT11-4-MAXRETRIES: Packet to client
   0040.96a0.3758 reached max retries, removing the client
Sep 22 10:35:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,
   Deauthenticating Station 0040.96a0.3758
   Reason: Previous authentication no longer valid
```

Сервер AP перенаправляет ответ на вызов от сервера radius клиенту. Клиент не может ответить и выполняет максимальное число повторных попыток, что приводит к ошибке в EAP и отмене аутентификации клиента в AP.

Отсутствует ответ от клиента

```
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
   Received server response: GET_CHALLENGE_RESPONSE
Sep 22 10:43:02: dot11_auth_dot1x_parse_aaa_resp:
   found eap pak in server response
Sep 22 10:43:02: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0040.96a0.3758
Sep 22 10:43:02: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 30 seconds
Sep 22 10:43:05: %DOT11-4-MAXRETRIES: Packet to client 0040.96a0.3758
   reached max retries, removing the client
Sep 22 10:43:05: Client 0040.96a0.3758 failed: reached maximum retries
```

Сервер Radius передает сообщение на AP, AP перенаправляет его клиенту, а клиент не отвечает. Таким образом, AP отменяет аутентификацию клиента после выполнения максимального числа повторных попыток. Клиент снова пытается послать запрос на идентификацию точке AP, но AP отклоняет запрос, так как клиент сделал максимальное число повторных попыток.

Отсутствует ответ от клиента

```
Sep 22 10:57:08: dot11_auth_dot1x_run_rfsm:
   Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
   Forwarding server message to client 0040.96a0.3758
Sep 22 10:57:08: dot11_auth_dot1x_send_response_to_client:
   Started timer client_timeout 30 seconds
Sep 22 10:57:08: %DOT11-6-ASSOC: Interface Dot11Radio0,
   Station arlit1ad1hd6j91 0040.96a0.3758 Reassociated KEY_MGMT[NONE]
Sep 22 10:57:10: %DOT11-4-MAXRETRIES: Packet to client
   0040.96a0.3758 reached max retries, removing the client
Sep 22 10:57:10: %DOT11-6-DISASSOC: Interface Dot11Radio0,
   Deauthenticating Station0040.96a0.3758 Reason:
   Previous authentication no longer valid
Sep 22 10:57:15: AAA/BIND(00001954): Bind i/f
Sep 22 10:57:15: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
   Sending identity request to 0040.96a0.3758
Sep 22 10:57:15: dot11_auth_dot1x_send_id_req_to_client:
   Client 0040.96a0.3758 timer started for 30 seconds
Sep 22 10:57:15: %DOT11-4-MAXRETRIES: Packet to client
   0040.96a0.3758 reached max retries, removing the client
Sep 22 10:57:15: Client 0040.96a0.3758 failed: reached maximum retries
```

Отладочные данные отладки **process** и/или **radius**, которые *предшествуют* сообщению о состоянии машин отображают подробную информацию об ошибке.

Дополнительные сведения о настройке EAP см. в разделе Аутентификация EAP с помощью сервера RADIUS.

Аутентификация протокола управления доступом к среде передачи (MAC)

Следующие процедуры отладки являются полезными для аутентификации MAC:

- **debug radius authentication** – во время использования внешнего сервера аутентификации, выходные данные этой отладки начинаются со слова: `RADIUS`.
- **debug dot11 aaa authenticator state-authen** – выходные данные этой команды отладки начинаются с текста: `dot11_auth_dot1x_`.

Представленные ниже отладочные данные содержат:

- Данные, выводимые во фрагментах взаимодействия с RADIUS, диалога аутентификации
- Сравнение данного MAC-адреса и аутентифицированного MAC-адреса

Если внешний сервер RADIUS используется с аутентификацией MAC-адреса, применяются отладочные данные RADIUS. Результатом является отображение фактического взаимодействия между сервером аутентификации и клиентом.

Если список MAC-адресов создан локально для устройства в качестве базы данных имен пользователя и паролей, выходные данные отображают только отладки **mac-authen**. Так как совпадение или несовпадение адресов определено, эти выходные данные отображаются.

Примечание. В MAC-адресе вводите буквенные символы в нижнем регистре.

В следующем примере отображена успешная аутентификация MAC-адреса в локальной базе данных:

Пример успешной аутентификации MAC

```
Apr  8 19:02:00.109: dot11_auth_mac_start: method_list: mac_methods
Apr  8 19:02:00.109: dot11_auth_mac_start: method_index: 0x4500000B, req: 0xA7626C
Apr  8 19:02:00.109: dot11_auth_mac_start: client->unique_id: 0x28
Apr  8 19:02:00.110: dot11_mac_process_reply: AAA reply for 0002.8aa6.304f PASSED
Apr  8 19:02:00.145: %DOT11-6-ASSOC: Interface Dot11Radio0, Station RKIBBE-W2K4
   0002.8aa6.304f Associated KEY_MGMT[NONE]
```

В следующем примере отображена ошибка аутентификации MAC в локальной базе данных:

Пример ошибки аутентификации EAP

```
Apr  8 19:01:22.336: dot11_auth_mac_start: method_list: mac_methods
Apr  8 19:01:22.336: dot11_auth_mac_start: method_index: 0x4500000B,
   req: 0xA7626C
Apr  8 19:01:22.336: dot11_auth_mac_start: client->unique_id: 0x27
Apr  8 19:01:22.337: dot11_mac_process_reply:
   AAA reply for 0002.8aa6.304f FAILED
Apr  8 19:01:22.337: %DOT11-7-AUTH_FAILED:
   Station 0002.8aa6.304f Authentication failed
```

Если не удалось выполнить аутентификацию MAC-адреса, проверьте точность ввода символов в MAC-адресе. Убедитесь, что буквенные символы MAC-адреса введены в нижнем регистре.

Дополнительные сведения о настройке аутентификации MAC см. в разделе Настройка типов аутентификации (Руководство по настройке ПО Cisco IOS для точек доступа Cisco Aironet версии 12.2(13)JA).

Защищенный доступ Wi-Fi (WPA)

Хотя защищенный доступ Wi-Fi (WPA) не является типом аутентификации, это согласованный протокол.

- WPA согласовывается между AP и картой клиента.
- Управление ключами WPA согласовывается после успешной аутентификации клиента с помощью сервера аутентификации.
- WPA согласовывается с парным временным ключом (PTK) и групповым временным ключом (GTK) в четырехстороннем

квитировании.

Примечание. Так как для WPA необходимо успешное выполнение основного EAP, проверьте возможность успешной аутентификации клиентов с помощью EAP перед обращением к WPA.

Следующие процедуры отладки являются полезными для согласований WPA:

- **debug dot11 aaa authenticator process** – выходные данные этой отладки начинаются с текста: `dot11_auth_dot1x_`.
- **debug dot11 aaa authenticator state-machine** – выходные данные этой команды отладки начинаются с текста: `dot11_auth_dot1x_run_rfsm`.

По отношению к другим типам аутентификации в данном документе отладочные данные WPA просты для чтения и анализа. Необходимо отправить сообщение PTK и получить соответствующий ответ. Потом необходимо отправить сообщение GTK и получить еще один ответ.

Если не отправить сообщения PTK или GTK, конфигурация или уровень ПО на сервере AP может быть неверными. Если ответы PTK или GTK от клиента не получены, проверьте конфигурацию или уровень ПО на запрашивающем устройстве WPA карты клиента.

Пример успешного согласования WPA

```
labap1200ip102#
Apr  7 16:29:57.908: dot11_dot1x_build_ptk_handshake:
   building PTK msg 1 for 0030.6527.f74a
Apr  7 16:29:59.190: dot11_dot1x_verify_ptk_handshake:
   verifying PTK msg 2 from 0030.6527.f74a
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning:
   Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning:
   Invalid key len (exp=0x20, act=0x0)
Apr  7 16:29:59.192: dot11_dot1x_build_ptk_handshake:
   building PTK msg 3 for 0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_ptk_handshake:
   verifying PTK msg 4 from 0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning:
   Invalid key info (exp=0x381, act=0x109
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning:
   Invalid key len (exp=0x20, act=0x0)
Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
   building GTK msg 1 for 0030.6527.f74a
Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
   dot11_dot1x_get_multicast_key len 32 index 1
Apr  7 16:29:59.788: dot11_dot1x_hex_dump: GTK:
   27 CA 88 7D 03 D9 C4 61 FD 4B BE 71 EC F7 43 B5 82 93 57 83
Apr  7 16:30:01.633: dot11_dot1x_verify_gtk_handshake:
   verifying GTK msg 2 from 0030.6527.f74a
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header:
   Warning: Invalid key info (exp=0x391, act=0x301
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning:
   Invalid key len (exp=0x20, act=0x0)
Apr  7 16:30:01.633: %DOT11-6-ASSOC: Interface Dot11Radio0,
   Station   0030.6527.f74a Associated KEY_MGMT[WPA]
labap1200ip102#
```

Дополнительные сведения о настройке WPA см. в разделе Обзор настройки WPA.

Административная аутентификация/аутентификация HTTP

Можно ограничить административный доступ к устройству для пользователей, внесенных в локальную базу данных имен пользователей и паролей, а также на внешний сервер аутентификации. Административный доступ поддерживается с помощью RADIUS и TACACS+.

Следующие процедуры отладки являются полезными для административной аутентификации.

- **debug radius authentication** или **debug tacacs authentication** – выходные данные этой отладки начинаются со слов: `RADIUS` или `TACACS`.
- **debug aaa authentication** – выходные данные этой отладки начинаются с текста: `AAA/AUTHEN`.
- **debug aaa authorization** – выходные данные этой отладки начинаются с текста: `AAA/AUTHOR`.

Представленные ниже отладочные данные содержат:

- Данные, выводимые во фрагментах взаимодействия с RADIUS или TACACS, диалога аутентификации
- Фактические согласования для аутентификации и авторизации между устройством и сервером аутентификации.

В данном примере отображена успешная административная аутентификация, если атрибут `Service-Type RADIUS` установлен на `Administrative`:

Пример успешной административной аутентификации с помощью атрибута Service-Type

```
Apr 13 19:43:08.030: AAA: parse name=tty2 idb type=-1 tty=-1
Apr 13 19:43:08.030: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0
   adapter=0 port=2 channel=0
Apr 13 19:43:08.031: AAA/MEMORY: create_user (0xA1BB6C) user='NULL' ruser='NULL'
   ds0=0 port='tty2' rem_addr='10.0.0.25' authen_type=ASCII service=LOGINN
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540): port='tty2'
   list='' action=LOGIN service=LOGIN
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540): using "default" list
Apr 13 19:43:08.031: AAA/AUTHEN/START (3200017540):
   Method=tac_admin (tacacs+)
Apr 13 19:43:08.032: TAC+: send AUTHEN/START packet ver=192 id=3200017540
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=ERROR
Apr 13 19:43:08.032: AAA/AUTHEN/START (3200017540):
   Method=rad_admin (radius)
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETUSER
Apr 13 19:43:08.032: AAA/AUTHEN/CONT (3200017540):
   continue_login (user='(undef)')
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETUSER
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Method=rad_admin (radius)
Apr 13 19:43:08.032: AAA/AUTHEN(3200017540): Status=GETPASS
Apr 13 19:43:08.033: AAA/AUTHEN/CONT (3200017540):
   continue_login (user='aironet')
Apr 13 19:43:08.033: AAA/AUTHEN(3200017540): Status=GETPASS
Apr 13 19:43:08.033: AAA/AUTHEN(3200017540): Method=rad_admin (radius)
Apr 13 19:43:08.033: RADIUS: Pick NAS IP for u=0xA1BB6C tableid=0
   cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 19:43:08.033: RADIUS: ustruct sharecount=1
Apr 13 19:43:08.034: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 19:43:08.034: RADIUS(00000000): Send Access-Request to 10.0.0.3:1645
   id 21646/48, len 76
Apr 13 19:43:08.034: RADIUS:  authenticator 91 A0 98 87 C1 FC F2 E7
   - E7 E4 57 DF 20 D0 82 27
Apr 13 19:43:08.034: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 19:43:08.034: RADIUS:  NAS-Port            [5]   6   2
Apr 13 19:43:08.035: RADIUS:  NAS-Port-Type       [61]  6   Virtual         [5]
Apr 13 19:43:08.035: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 19:43:08.035: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 19:43:08.035: RADIUS:  User-Password       [2]   18  *
Apr 13 19:43:08.042: RADIUS: Received from id 21646/48 10.0.0.3:1645,
   Access-Accept, len 62
Apr 13 19:43:08.042: RADIUS:  authenticator C9 32 E7 8F 97 5F E6 4C
   - 6B 90 71 EE ED 2C 2B 2B
Apr 13 19:43:08.042: RADIUS:  Service-Type        [6]   6
   Administrative            [6]
Apr 13 19:43:08.042: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 19:43:08.042: RADIUS:  Class               [25]  30
Apr 13 19:43:08.043: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 36
```

```
   [CISCOACS:0000366]
Apr 13 19:43:08.043: RADIUS:   39 2F 30 61 30 30 30 30 36 36 2F 32
   [9/0a000066/2]
Apr 13 19:43:08.044: RADIUS: saved authorization data for user A1BB6C at B0C260
Apr 13 19:43:08.044: AAA/AUTHEN(3200017540): Status=PASS
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147):
   Port='tty2' list='' service=EXEC
Apr 13 19:43:08.044: AAA/AUTHOR/HTTP: tty2(1763745147) user='aironet'
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV service=shell
Apr 13 19:43:08.044: tty2 AAA/AUTHOR/HTTP(1763745147): send AV cmd*
Apr 13 19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): found list "default"
Apr 13 19:43:08.045: tty2 AAA/AUTHOR/HTTP(1763745147): Method=tac_admin (tacacs+)
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): user=aironet
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): send AV service=shell
Apr 13 19:43:08.045: AAA/AUTHOR/TAC+: (1763745147): send AV cmd*
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147): Post authorization status = ERROR
Apr 13 19:43:08.046: tty2 AAA/AUTHOR/HTTP(1763745147):
   Method=rad_admin (radius)
Apr 13 19:43:08.046: AAA/AUTHOR (1763745147):
   Post authorization status = PASS_ADD
Apr 13 19:43:08.443: AAA/MEMORY: free_user (0xA1BB6C) user='aironet'
   ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII service=LOGIN
```

В данном примере отображена успешная административная аутентификация с использованием специфических для поставщика атрибутов для отправки оператора "priv-level".

Пример успешной административной аутентификации с помощью атрибута Vendor-Specific

```
Apr 13 19:38:04.699: RADIUS: cisco AVPair ""shell:priv-lvl=15""
   not applied for shell
Apr 13 19:38:04.699: AAA/AUTHOR (380584213): Post authorization status
   = PASS_ADD
Apr 13 19:38:04.802: AAA/MEMORY: free_user (0xAA0E38) user='aironet'
   ruser='NULL' port='tty3' rem_addr='10.0.0.25' authen_type=ASCII
   service=LOGIN
Apr 13 19:38:04.901: AAA: parse name=tty3 idb type=-1 tty=-1
Apr 13 19:38:04.901: AAA: name=tty3 flags=0x11 type=5 shelf=0 slot=0
   adapter=0  port=3 channel=0
Apr 13 19:38:04.902: AAA/MEMORY: create_user (0xAA23BC) user='NULL'
   ruser='NULL' ds0=0 port='tty3' rem_addr='10.0.0.25'
   authen_type=ASCII service=LOGIN
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): port='tty3' list=''
   action=LOGIN service=LOGIN
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): using "default" list
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): Method=tac_admin (tacacs+)
Apr 13 19:38:04.902: TAC+: send AUTHEN/START packet ver=192 id=1346300140
Apr 13 19:38:04.902: AAA/AUTHEN(1346300140): Status=ERROR
Apr 13 19:38:04.902: AAA/AUTHEN/START (1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.902: AAA/AUTHEN(1346300140): Status=GETUSER
Apr 13 19:38:04.903: AAA/AUTHEN/CONT (1346300140): continue_login
   (user='(undef)')
Apr 13 19:38:04.903: AAA/AUTHEN(1346300140): Status=GETUSER
Apr 13 19:38:04.903: AAA/AUTHEN(1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS
Apr 13 19:38:04.904: AAA/AUTHEN/CONT (1346300140): continue_login
   (user='aironet')
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Status=GETPASS
Apr 13 19:38:04.904: AAA/AUTHEN(1346300140): Method=rad_admin (radius)
Apr 13 19:38:04.904: RADIUS: Pick NAS IP for u=0xAA23BC tableid=0
   cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 19:38:04.904: RADIUS: ustruct sharecount=1
Apr 13 19:38:04.904: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 19:38:04.925: RADIUS(00000000): Send Access-Request to
   10.0.0.3:1645 id 21646/3, len 76
Apr 13 19:38:04.926: RADIUS:  authenticator 0C DD 2B B7 CA 5E 7C B9
   - 46 90 FD 7A FD 56 3F 07
Apr 13 19:38:04.926: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 19:38:04.926: RADIUS:  NAS-Port            [5]   6   3
Apr 13 19:38:04.926: RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
Apr 13 19:38:04.926: RADIUS:  User-Name           [1]   9   "aironet"
Apr 13 19:38:04.926: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 19:38:04.926: RADIUS:  User-Password       [2]   18  *
Apr 13 19:38:04.932: RADIUS: Received from id 21646/3 10.0.0.3:1645,
   Access-Accept, len 89
Apr 13 19:38:04.933: RADIUS:  authenticator FA A4 31 49 51 87 9D CA
```

```
   - 9D F7 B3 9B EF C2 8B 7E
Apr 13 19:38:04.933: RADIUS:  Vendor, Cisco       [26]  27
Apr 13 19:38:04.933: RADIUS:   Cisco AVpair     [1]   21  ""shell:priv-lvl=15""
Apr 13 19:38:04.934: RADIUS:  Service-Type        [6]   6   Login       [1]
Apr 13 19:38:04.934: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 19:38:04.934: RADIUS:  Class               [25]  30
Apr 13 19:38:04.934: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 33
   [CISCOACS:0000363]
Apr 13 19:38:04.934: RADIUS:   61 2F 30 61 30 30 30 30 36 36 2F 33
   [a/0a000066/3]
Apr 13 19:38:05.634: AAA/AUTHOR (3854191802): Post authorization
   status = PASS_ADD
Apr 13 19:38:05.917: AAA/MEMORY: free_user (0xA9D054) user='aironet'
   ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
   service=LOGIN priv=0
```

Наиболее распространенная проблема административной аутентификации – это ошибка в настройке сервера аутентификации для отправки соответствующих атрибутов privilege-level или административных атрибутов service-type. В данном примере не удалось выполнить административную аутентификацию, так как атрибуты privilege-level или административные атрибуты service-type не были отправлены:

Без атрибутов Vendor-Specific или Service-Type

```
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): Port='tty3'
   list='' service=EXEC
Apr 13 20:02:59.516: AAA/AUTHOR/HTTP: tty3(2007927065) user='aironet'
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): send AV service=shell
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): send AV cmd*
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): found list "default"
Apr 13 20:02:59.516: tty3 AAA/AUTHOR/HTTP(2007927065): Method=tac_admin (tacacs+)
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): user=aironet
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send AV service=shell
Apr 13 20:02:59.516: AAA/AUTHOR/TAC+: (2007927065): send AV cmd*
Apr 13 20:02:59.516: AAA/AUTHOR (2007927065): Post authorization status = ERROR
Apr 13 20:02:59.517: tty3 AAA/AUTHOR/HTTP(2007927065): Method=rad_admin (radius)
Apr 13 20:02:59.517: AAA/AUTHOR (2007927065): Post authorization status = PASS_ADD
Apr 13 20:02:59.561: AAA/MEMORY: free_user (0xA756E8) user='aironet'
   ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
   service=LOGIN priv=0  vrf= (id=0)
Apr 13 20:02:59.620: AAA/MEMORY: free_user (0x9E5B04) user='aironet'
   ruser='NULL'  port='tty3' rem_addr='10.0.0.25' authen_type=ASCII
   service=LOGIN priv=0 vrf= (id=0)
Apr 13 20:03:04.501: AAA: parse name=tty2 idb type=-1 tty=-1
Apr 13 20:03:04.501: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0 adapter=0
   port=2 channel=0
Apr 13 20:03:04.502: AAA/MEMORY: create_user (0xA9C7A4) user='NULL'
   ruser='NULL' ds0=0 port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
   service=LOGIN priv=0
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): port='tty2' list=''
   action=LOGIN service=LOGIN
Apr 13 20:03:04.502: AAA/AUTHEN/START (377202642): using "default" list
Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642): Method=tac_admin (tacacs+)
Apr 13 20:03:04.503: TAC+: send AUTHEN/START packet ver=192 id=377202642
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=ERROR
Apr 13 20:03:04.503: AAA/AUTHEN/START (377202642): Method=rad_admin (radius)
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETUSER
Apr 13 20:03:04.503: AAA/AUTHEN/CONT (377202642): continue_login (user='(undef)')
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETUSER
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Method=rad_admin (radius)
Apr 13 20:03:04.503: AAA/AUTHEN(377202642): Status=GETPASS
Apr 13 20:03:04.504: AAA/AUTHEN/CONT (377202642): continue_login (user='aironet')
Apr 13 20:03:04.504: AAA/AUTHEN(377202642): Status=GETPASS
Apr 13 20:03:04.504: AAA/AUTHEN(377202642): Method=rad_admin (radius)
Apr 13 20:03:04.504: RADIUS: Pick NAS IP for u=0xA9C7A4 tableid=0
   cfg_addr=10.0.0.102 best_addr=0.0.0.0
Apr 13 20:03:04.505: RADIUS: ustruct sharecount=1
Apr 13 20:03:04.505: Radius: radius_port_info() success=1 radius_nas_port=1
Apr 13 20:03:04.505: RADIUS(00000000): Send Access-Request to 10.0.0.3:1645
   id 21646/59, len 76
Apr 13 20:03:04.505: RADIUS:  authenticator 0F BD 81 17 8F C5 1C B4
   - 84 1C 66 4D CF D4 96 03
Apr 13 20:03:04.505: RADIUS:  NAS-IP-Address      [4]   6   10.0.0.102
Apr 13 20:03:04.506: RADIUS:  NAS-Port            [5]   6   2
Apr 13 20:03:04.506: RADIUS:  NAS-Port-Type       [61]  6   Virtual           [5]
Apr 13 20:03:04.506: RADIUS:  User-Name           [1]   9   "aironet"
```

```
Apr 13 20:03:04.506: RADIUS:  Calling-Station-Id  [31]  11  "10.0.0.25"
Apr 13 20:03:04.507: RADIUS:  User-Password       [2]   18  *
Apr 13 20:03:04.513: RADIUS: Received from id 21646/59 10.0.0.3:1645,
   Access-Accept, len 56
Apr 13 20:03:04.513: RADIUS:  authenticator BB F0 18 78 33 D0 DE D3
   - 8B E9 E0 EE 2A 33 92 B5
Apr 13 20:03:04.513: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
Apr 13 20:03:04.513: RADIUS:  Class               [25]  30
Apr 13 20:03:04.514: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 33 36 38
   [CISCOACS:0000368]
Apr 13 20:03:04.514: RADIUS:   33 2F 30 61 30 30 30 30 36 36 2F 32
   [3/0a000066/2]
Apr 13 20:03:04.515: RADIUS: saved authorization data for user A9C7A4 at A9C99C
Apr 13 20:03:04.515: AAA/AUTHEN(377202642): Status=PASS
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): Port='tty2' list=''
   service=EXEC
Apr 13 20:03:04.515: AAA/AUTHOR/HTTP: tty2(2202245138) user='aironet'
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): send AV service=shell
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): send AV cmd*
Apr 13 20:03:04.515: tty2 AAA/AUTHOR/HTTP(2202245138): found list "default"
Apr 13 20:03:04.516: tty2 AAA/AUTHOR/HTTP(2202245138): Method=tac_admin (tacacs+)
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): user=aironet
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send AV service=shell
Apr 13 20:03:04.516: AAA/AUTHOR/TAC+: (2202245138): send AV cmd*
Apr 13 20:03:04.517: AAA/AUTHOR (2202245138): Post authorization status = ERROR
Apr 13 20:03:04.517: tty2 AAA/AUTHOR/HTTP(2202245138): Method=rad_admin (radius)
Apr 13 20:03:04.517: AAA/AUTHOR (2202245138): Post authorization status
   = PASS_ADD
Apr 13 20:03:04.619: AAA/MEMORY: free_user (0xA9C7A4) user='aironet'
   ruser='NULL' port='tty2' rem_addr='10.0.0.25' authen_type=ASCII
   service=LOGIN priv=0 vrf=
```

Дополнительные сведения о настройке административной аутентификации см. в разделе Администрирование точек доступа (Руководство по настройке программного обеспечения Cisco IOS Software для точек доступа Cisco Aironet версии 12.2(13)JA).

Дополнительные сведения о настройке административной привилегии для пользователей на сервере аутентификации см. в разделе Пример конфигурации: локальная аутентификация для пользователей сервера HTTP. Ознакомьтесь с разделом, соответствующим протоколу аутентификации, который вы используете.

Дополнительные сведения

- **Руководство по настройке ПО Cisco IOS для точек доступа Cisco Aironet версии 12.2(13)JA**
- **Аутентификация EAP с помощью сервера RADIUS**
- **Аутентификация LEAP с помощью локального сервера RADIUS**
- **Вопросы и ответы по безопасности беспроводных устройств Cisco Aironet**
- **Пример настройки AP беспроводных доменных служб в качестве сервера AAA**
- **Cisco Systems – техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107684/debug_authen.shtml