Руководство по настройке проверки подлинности LEAP/MAC

Содержание

Введение

Этот документ предоставляет пример конфигурации для аутентификации Легковесного расширяемого протокола аутентификации (LEAP) на точке доступа IOS®-based, которая служит беспроводным клиентам, а также действует как локальный сервер RADIUS. Это применимо к точке доступа IOS, которая выполняется 12.2 (11) JA или позже.

Предварительные условия

Требования

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

- Знакомство с IOS GUI или CLI
- Знакомство с основами аутентификации LEAP

Компоненты

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

- Точка доступа Cisco Aironet серии 1240AG
- Программное обеспечение Cisco IOS версии 12.3 (8) JA2
- 802.11 Cisco Aironet a/b/g/Беспроводной адаптер, который выполняет служебную программу рабочего стола Aironet 3.6.0.122
- Предположим, что в сети только одна VLAN

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.

Обзор функции локального сервера RADIUS

Обычно внешний сервер RADIUS используется для аутентификации пользователей. В некоторых случаях это не Осуществимое решение. В этих ситуациях точка доступа может быть сделана действовать как сервер RADIUS. Здесь, пользователи аутентифицируются против локальной базы данных, настроенной в точке доступа. Это называют функцией Локального сервера RADIUS. Можно также сделать другие точки доступа в использовании сети функцией Локального сервера RADIUS на точке доступа. Для получения дополнительной информации об этом обратитесь к Настройке Другие точки доступа Использовать Локальный аутентификатор.

Настройка

Конфигурация описывает, как настроить LEAP и Локальную Функцию сервера RADIUS на точке доступа. Функция локального RADIUS-сервера была впервые представлена в программном обеспечении Cisco IOS релиза 12.2(11)JA. См. Аутентификацию LEAP с сервером RADIUS для общих сведений о том, как настроить LEAP с внешним сервером RADIUS.

Как и большинство алгоритмов аутентификации, основанных на вводе пароля, Cisco LEAP чувствителен к словарным атакам. Речь не идет о новом виде атаки или новом уязвимом месте Cisco LEAP. Для того, чтобы смягчить словарные атаки, необходимо разработать политику стойкого пароля, которая включает в себя устойчивые пароли и частую их смену. Для получения дополнительной информации о словарных атаках и защите от них обратитесь к документу Словарные атаки на Cisco LEAP.

Этот документ принимает эту конфигурацию и для CLI и для GUI:

1. IP-адрес точки доступа **10.77.244.194**.
2. Используемый SSID является **Cisco**, который сопоставлен с **VLAN 1**.
3. Имена пользователей являются **user1** и **user2**, которые сопоставлены с **Testuser** группы.

Конфигурация интерфейса командой строки CLI

Точка доступа

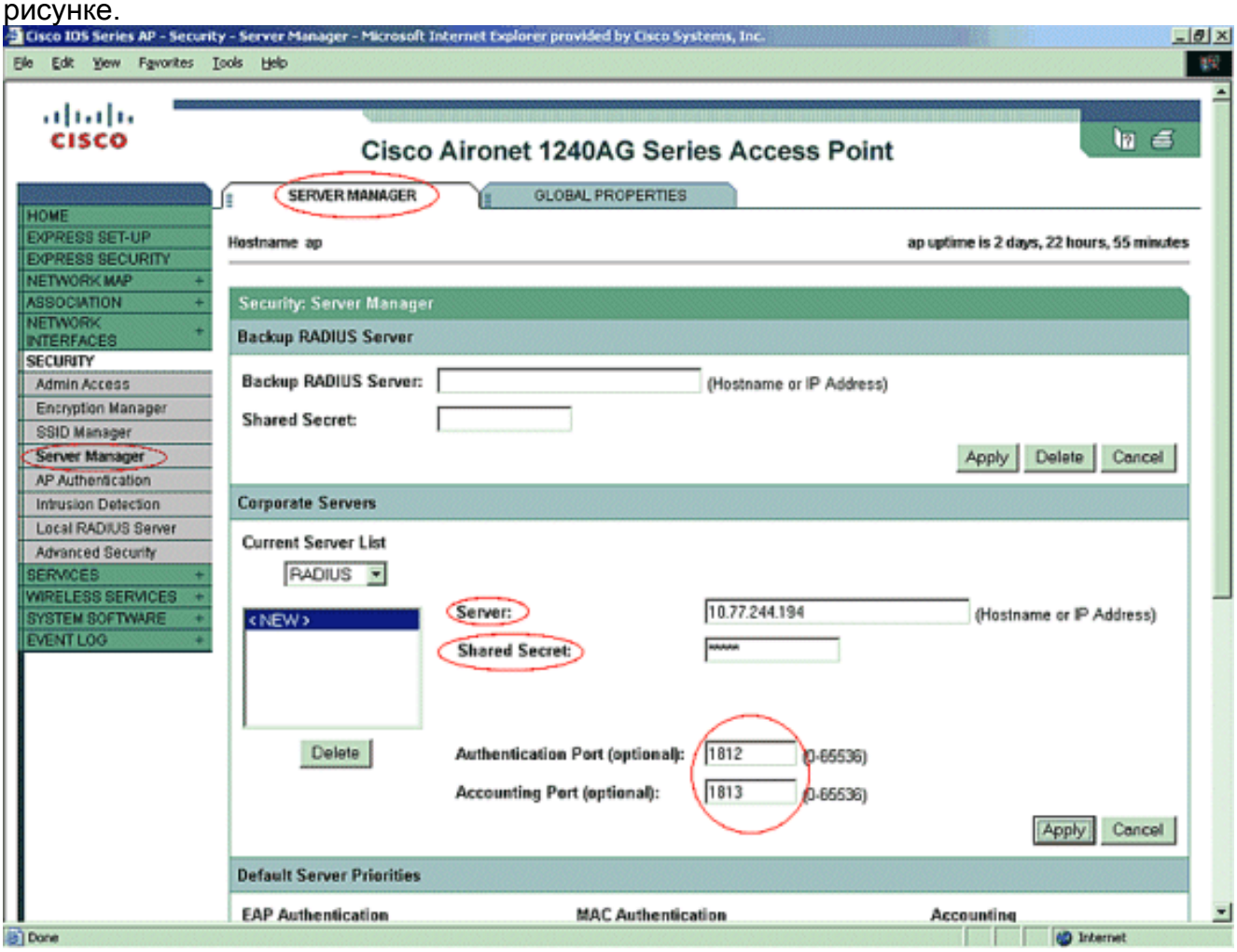
```
ap#show running-config Building configuration... . . .
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap server
10.77.244.194 auth-port 1812 acct-port 1813 !--- A
server group for RADIUS is created called "rad_eap" !---
that uses the server at 10.77.244.194 on ports 1812 and
1813. . . . aaa authentication login eap_methods group
rad_eap !--- Authentication [user validation] is to be
done for !--- users in a group called "eap_methods" who
use server group "rad_eap". . . . ! bridge irb !
interface Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
12345678901234567890123456 transmit-key !This step is
optional----!--- This value seeds the initial key for
use with !--- broadcast [255.255.255.255] traffic. If
more than one VLAN is !--- used, then keys must be set
for each VLAN. encryption vlan 1 mode wep mandatory !---
This defines the policy for the use of Wired Equivalent
Privacy (WEP). !--- If more than one VLAN is used, !---
the policy must be set to mandatory for each VLAN.
broadcast-key vlan 1 change 300 !--- You can also enable
Broadcast Key Rotation for each vlan and Specify the
time after which Brodacst key is changed. If it is
disabled Broadcast Key is still used but not changed.
ssid cisco vlan 1 !--- Create a SSID Assign a vlan to
this SSID authentication open eap eap_methods
authentication network-eap eap_methods !--- Expect that
users who attach to SSID "cisco" !--- request
authentication with the type 128 Open EAP and Network
EAP authentication !--- bit set in the headers of those
requests, and group those users into !--- a group called
"eap_methods." ! speed basic-1.0 basic-2.0 basic-5.5
basic-11.0 rts threshold 2312 channel 2437 station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled . . .
interface FastEthernet0 no ip address no ip route-cache
duplex auto speed auto bridge-group 1 no bridge-group 1
source-learning bridge-group 1 spanning-disabled !
interface BVI1 ip address 10.77.244.194 255.255.255.0 !-
-- The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.77.244.194 key shared_secret !---
Identifies itself as a RADIUS server, reiterates !---
"localness" and defines the key between the server
(itself) and the access point. ! group testuser !---
Groups are optional. ! user user1 nthash password1 group
testuser !--- Individual user user user2 nthash
password2 group testuser !--- Individual user !--- These
individual users comprise the Local Database ! radius-
server host 10.77.244.194 auth-port 1812 acct-port 1813
key shared_secret !--- Defines where the RADIUS server
is and the key between !--- the access point (itself)
and the server. radius-server retransmit 3 radius-server
attribute 32 include-in-access-req format %h radius-
```

```
server authorization permit missing Service-Type radius-
server vsa send accounting bridge 1 route ip ! ! line
con 0 line vty 5 15 ! end
```

Конфигурация графического интерфейса пользователя (GUI)

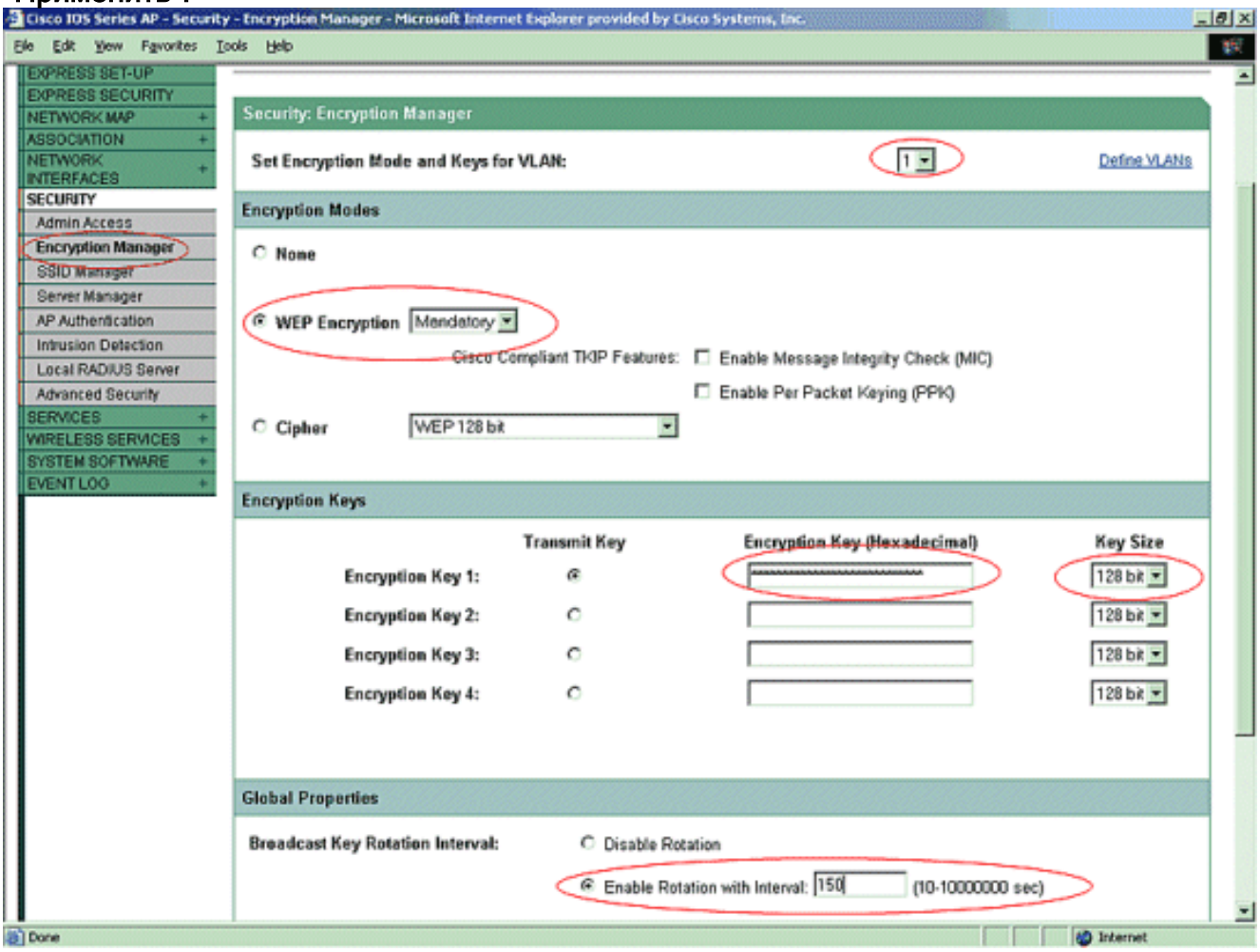
Выполните эти шаги для настройки функции Локального сервера RADIUS с GUI:

1. Из меню в левой стороне выберите вкладку Server Manager в соответствии с Меню системы безопасности.Настройте сервер и упомяните IP-адрес этой точки доступа, которая является 10.77.244.194 в данном примере.Упомяните номера портов 1812 и 1813, на которых слушает Локальный сервер RADIUS.Задайте общий секретный ключ, который будет использоваться с Локальным сервером RADIUS как показано на рисунке.

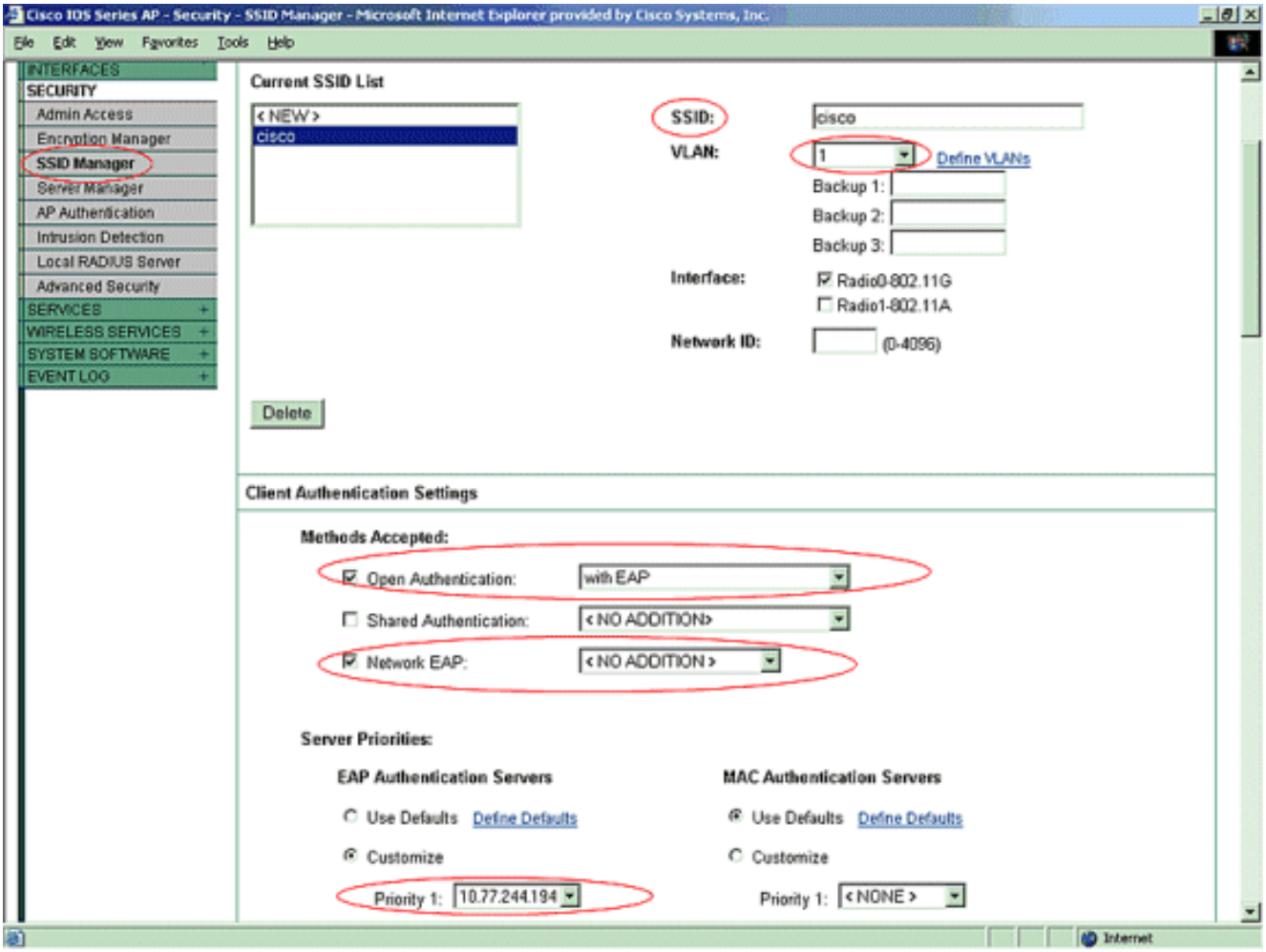


2. Из меню в левой стороне нажмите вкладку Encryption Manager в соответствии с Меню системы безопасности.Задайте VLAN, которая будет применена.Установите использование шифрования WEP.Укажите, что его использование ОБЯЗАТЕЛЬНО.Инициализируйте любой Ключ WEP с 26-разрядным шестнадцатеричным символом. Этот ключ используется для шифрования широковещания и пакетов групповой адресации. Этот шаг не является обязательным.Установить размер ключа равным 128 бит. Можно также выбрать 40 битов. В этом случае размер Ключа WEP в предыдущем шаге должен быть 10-разрядным шестнадцатеричным символом. Этот шаг не является обязательным.Можно также включить ротацию (широковещательных) ключей и задать время, после которого изменен широковещательный ключ. Если это отключено,

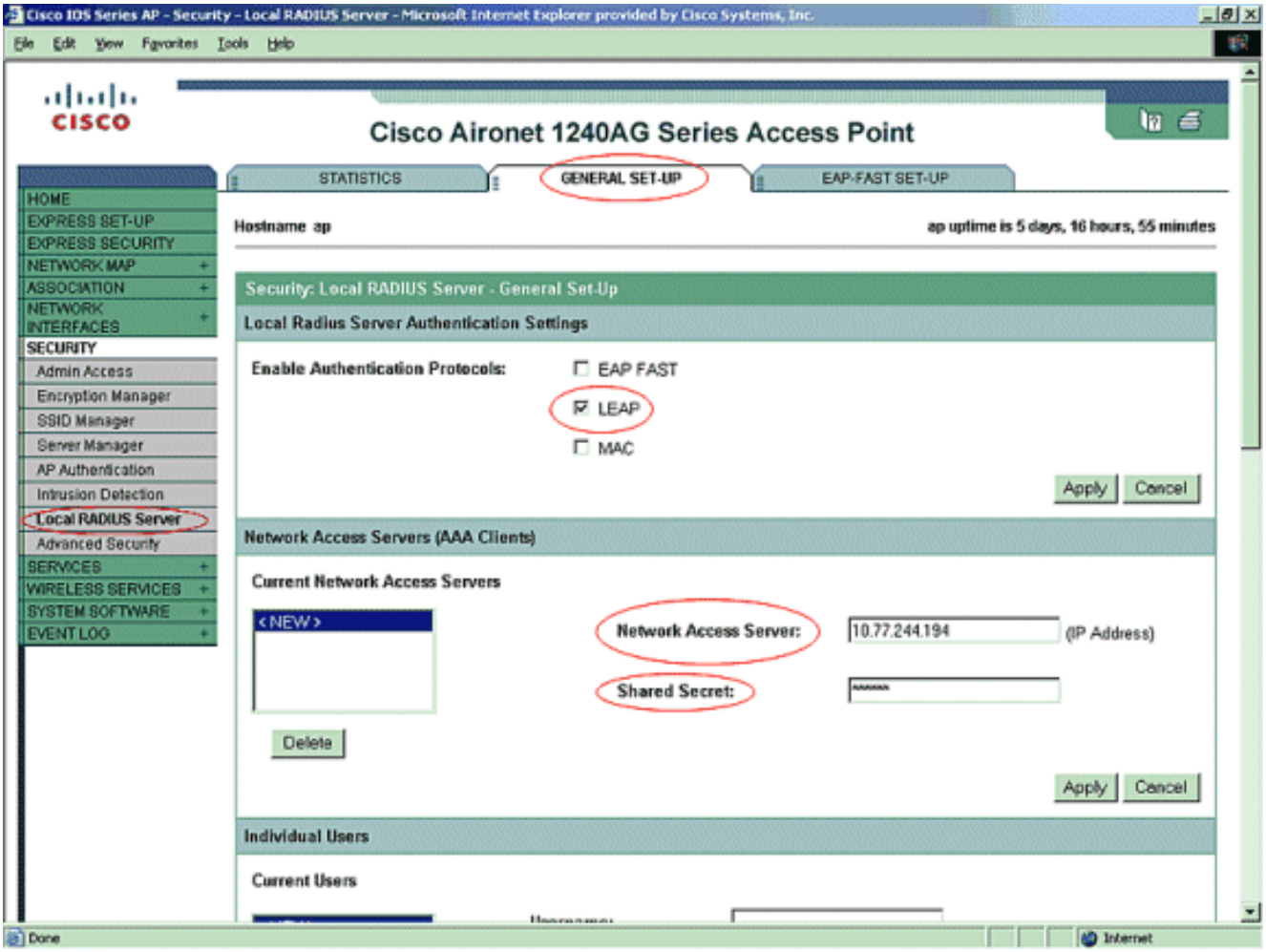
широковещательный ключ все еще используется, но не изменяется. Этот шаг не является обязательным.**Примечание:** Эти шаги повторены для каждой VLAN, которая использует Аутентификацию LEAP**Щелкните "Применить".**



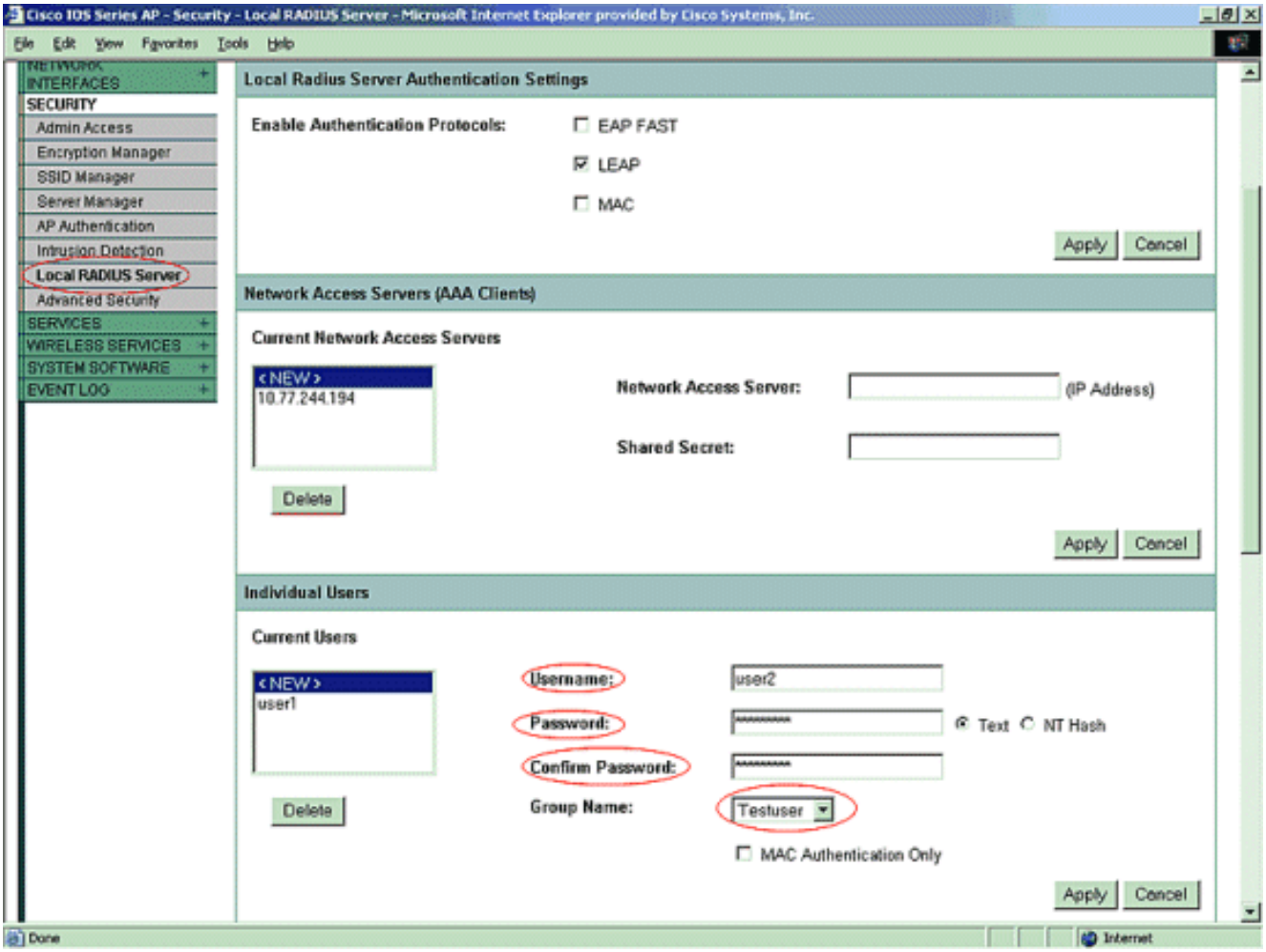
3. В соответствии с Меню системы безопасности, от вкладки SSID Manager, выполняют эти действия:**Примечание:** Можно добавить дополнительные опции и управление ключами позже, как только вы подтверждаете, что основная конфигурация работает правильно.Определить новый SSID и связать его с VLAN. В данном примере SSID привязан к VLAN 1.**Установить флажок Open Authentication (With EAP).Установить флажок Network EAP (No Addition).**От **Приоритетов Сервера> Серверы Аутентификации eap**, выберите **Customize**; выберите IP-адрес этой **точки доступа forPriority 1.Щелкните "Применить".**



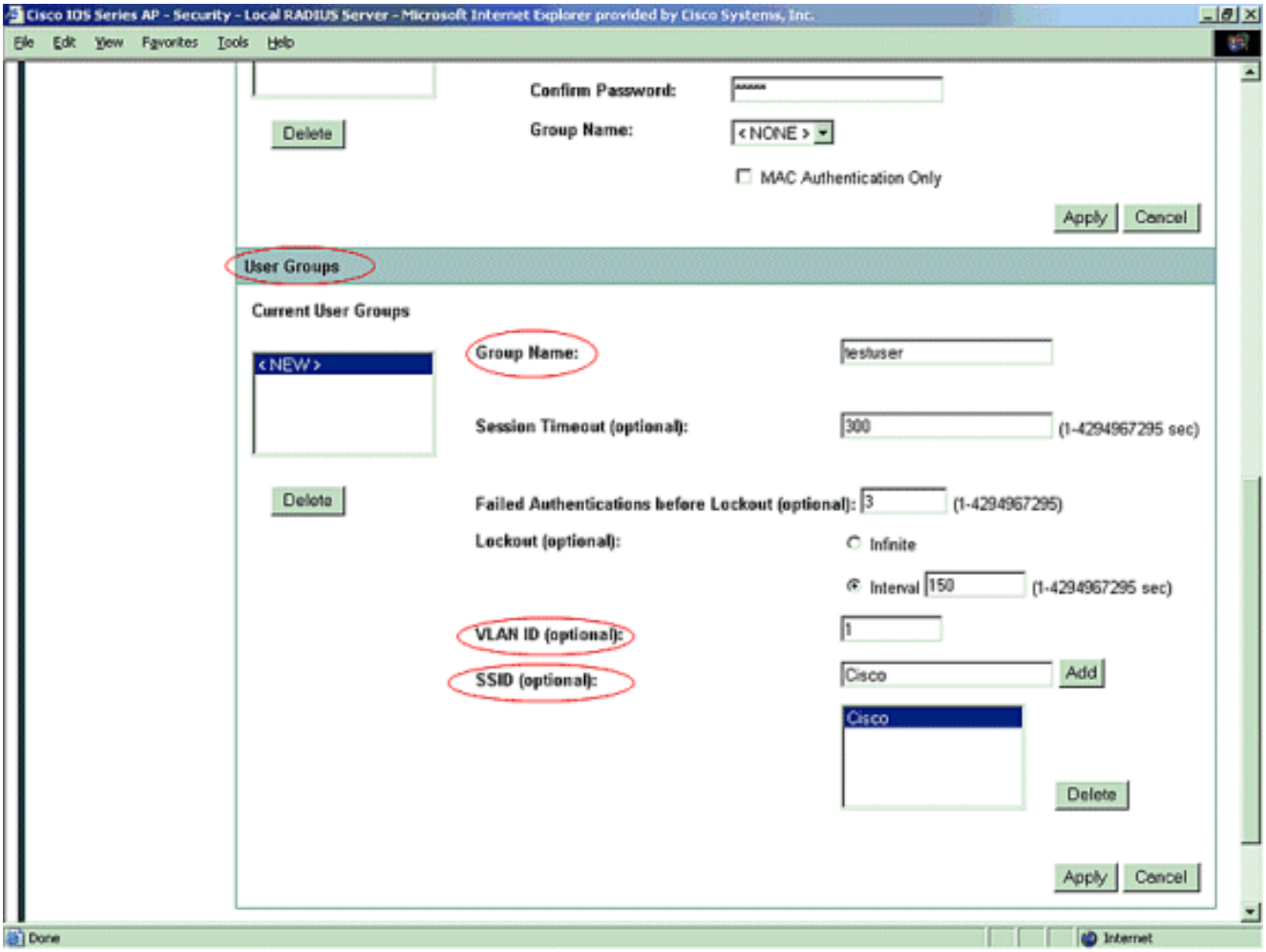
4. Под Безопасностью нажмите Local RADIUS Server от вкладки General Set-UPПри Локальных Параметрах настройки аутентификации сервера RADIUS проверьте **LEAP**, чтобы удостовериться, что приняты запросы Аутентификации LEAP.Определите IP-адрес и общий секретный пароль сервера RADIUS. Для Локального сервера RADIUS это - IP-адрес этого AP (10.77.244.194).**Щелкните "Применить".**



5. Прокрутите вниз от Локального сервера RADIUS под вкладкой General Setup и определите отдельных пользователей с их именами пользователя и паролями. Дополнительно, пользователи могут быть привязаны к Группам, который определен в следующем шаге. Это удостоверяется, что только некоторые пользователи входят в SSID.**Примечание:** Локальная База данных RADIUS состоит из этих отдельных имен пользователя и
паролей.



6. Перейдите далее вниз на той же странице, снова от Локального сервера RADIUS под Общей подзакладкой Настройки Группам пользователей; определите группы пользователей и привяжите их к VLAN или SSID.



Примечание: !--- Группы являются необязательными. Атрибуты группы не передаются в Active Directory и имеют значение только локально. Группы можно будет добавить позже, после того, как будет подтверждено, что основная конфигурация работает правильно.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- **show radius local-server statistics – эта команда отображает статистику, собранную локальным аутентификатором.**

```
Successes              : 27          Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.77.244.194
Successes              : 27          Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
Auto provision success : 0           Auto provision failure : 0
PAC refresh            : 0           Invalid PAC received   : 0

Username                    Successes  Failures  Blocks
user1                              27         0       0
```

- **show radius server-group all – эта команда отображает список всех настроенных**

серверных групп RADIUS в точке доступа.

Устранение неполадок

Процедура устранения неполадок

В данном разделе представлена информация по устранению проблем, касающихся данной конфигурации.

1. **Для того, чтобы исключить возможность влияния радиочастотных помех на успешную аутентификацию, необходимо установить метод на SSID равным Open для того, чтобы временно отключить аутентификацию.В GUI на странице SSID Manager снять флажок Network-EAP и нажать Open.В командной строке использовать команды authentication open и no authentication network-eap eap_methods.**Если клиент будет успешно сопоставлен, то радиочастота не вызовет проблем сопоставления.
2. Убедитесь, что все общие пароли синхронизированы. `Radius-server host` линий `x. x. x. x acct- x x <shared_secret>` и `nas x. x. x. x <shared_secret>` должен содержать тот же общий секретный пароль.
3. Необходимо удалить все группы пользователей и все настройки, связанные с ними. Ингода могут возникать конфликты между группами пользователей, определенными точкой доступа, и группами пользователей на домене.

Команды для устранения неполадок

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

- **средство проверки подлинности debug dot11 aaa все** — Эта отладка показывает различные согласования, что клиент проходит, поскольку клиент связывается и аутентифицируется через 802.1x или процесс EAP с точки зрения Средства проверки подлинности (точка доступа). Данная функция отладки была представлена в ПО Cisco IOS версии 12.2(15)JA. Эта команда заметила отладочную команду dot11 aaa dot1x all в этой и последующих версиях.

```
 *Mar  1 00:26:03.097: dot11_auth_add_client_entry:
   Create new client 0040.96af.3e93 for application 0x1
 *Mar  1 00:26:03.097: dot11_auth_initialize_client:
   0040.96af.3e93 is added to the client list for application 0x1
-----------------------------------------------
   Lines Omitted for simplicity ------------------
*Mar  1 00:26:03.098: dot11_auth_dot1x_start:
   in the dot11_auth_dot1x_start


*Mar  1 00:26:03.132: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93
*Mar  1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client:
   Sending identity request to 0040.96af.3e93(client) *Mar 1 00:26:03.133: *Mar 1
00:26:03.099: dot11_auth_dot1x_send_id_req_to_client: Client 0040.96af.3e93 timer started
for 30 seconds *Mar 1 00:26:03.132: dot11_auth_parse_client_pak: Received EAPOL packet from
0040.96af.3e93 ----------------------------------------------- Lines Omitted--------------
------------------- *Mar 1 00:26:03.138: EAP code: 0x2 id: 0x1 length: 0x000A type: 0x1
01805BF0: 0100000A 0201000A 01757365 7231 .........user1(User Name of the client) *Mar1
```

00:26:03.146: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93 *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server: **Sending client 0040.96af.3e93 data to server** *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds ---------- Lines Omitted---------- *Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp: **Received server response:GET_CHALLENGE_RESPONSE** *Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp: found session timeout 10 sec *Mar 1 00:26:03.150: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96af.3e93 *Mar 1 00:26:03.150: dot11_auth_dot1x_send_response_to_client: **Forwarding server message to client 0040.96af.3e93** ---------- Lines Omitted---------- *Mar 1 00:26:03.151: dot11_auth_send_msg: **Sending EAPOL to requestor** *Mar 1 00:26:03.151: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 10 seconds *Mar 1 00:26:03.166: dot11_auth_parse_client_pak: **Received EAPOL packet*(User Credentials)* from 0040.96af.3e93** *Mar 1 00:26:03.166: EAP code: 0x2 id: 0x11 length: 0x0025 type: 0x11 01805F90: 01000025 02110025...%...%01805FA0: 11010018 7B75E719 C5F3575E EFF64B27 **....{ug.EsW^ovK'** Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93 *Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: **Sending client 0040.96af.3e93 data *(User Credentials)* to server** *Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds ---------- ---------- Lines Omitted---------- *Mar 1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp: **Received server response: PASS** *Mar 1 00:26:03.197: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93 *Mar 1 00:26:03.197: dot11_auth_dot1x_send_response_to_client: **Forwarding server message*(Pass Message)* to client** ---------- Lines Omitted---------- *Mar 1 00:26:03.198: dot11_auth_send_msg: Sending EAPOL to requestor *Mar 1 00:26:03.199: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 second *Mar 1 00:26:03.199: dot11_auth_send_msg: **client authenticated 0040.96af.3e93,** node_type 64 for application 0x1 *Mar 1 00:26:03.199: dot11_auth_delete_client_entry: 0040.96af.3e93 is deleted for application 0x1 *Mar 1 00:26:03.200: %DOT11-6-ASSOC: **Interface Dot11Radio0, Station *Station Name* 0040.96af.3e93 Associated KEY_MGMT[NONE]**

- debug radius authentication — Эта отладка показывает Согласования RADIUS между сервером и клиентом, оба из которых, в этом случае, являются точкой доступа.
- клиент debug radius local-server — Эта отладка показывает аутентификацию клиента с точки зрения сервера RADIUS.

*Mar 1 00:30:00.742: RADIUS(0000001A):
Send Access-Request*(Client's User Name)* to 10.77.244.194:1812*(Local Radius Server)* id 1645/65, len 128 *Mar 1 00:30:00.742: RADIUS: **User-Name [1] 7 "user1"** *Mar 1 00:30:00.742: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0" *Mar 1 00:30:00.743: RADIUS: **Calling-Station-Id [31] 16 "0040.96af.3e93" *(Client)*** *Mar 1 00:30:00.743: RADIUS: Service-Type [6] 6 Login [1] *Mar 1 00:30:00.743: RADIUS: Message-Authenticato[80] *Mar 1 00:30:00.743: RADIUS: 23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B [#.?B??rK(DnzX??{] *Mar 1 00:30:00.743: RADIUS: EAP-Message [79] 12 *Mar 1 00:30:00.743: **RADIUS: 02 02 00 0A 01 75 73 65 72 31 [?????user1]** *Mar 1 00:30:00.744: RADIUS: NAS-Port-Type [61] 6 802.11 wireless ---------- ---------- Lines Omitted For Simplicity---------- *Mar 1 00:30:00.744: RADIUS: **NAS-IP-Address [4] 6 10.77.244.194*(Access Point IP)*** *Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap" ---------- Lines Omitted---------- ---------- *Mar 1 00:30:00.745: RADIUS: **Received from id 1645/65 10.77.244.194:1812, Access-Challenge**, len 117 *Mar 1 00:30:00.746: RADIUS: 75 73 65 72 31 **[user1]** *Mar 1 00:30:00.746: RADIUS: Session-Timeout [27] 6 10 *Mar 1 00:30:00.747: RADIUS: State [24] 50 *Mar 1 00:30:00.747: RADIUS: BF 2A A0 7C 82 65 76 AA 00 00 00 00 00 00 00 00 [?*?|?ev?????????] ---------- Lines Omitted for simplicity ---------- *Mar 1 00:30:00.756: RADIUS/ENCODE(0000001A):Orig. component type = DOT11 *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: ssid [264] 5 *Mar 1 00:30:00.756: RADIUS: 63 69 73 [cis] *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: interface [157] 3 *Mar 1 00:30:00.756: RADIUS: 32 [2] *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A): acct_session_id: 26 *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.779: RADIUS(0000001A): **Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189** *Mar 1 00:30:00.779: RADIUS: authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F *Mar 1 00:30:00.779: RADIUS: User-Name [1] 7 "user1" *Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400 *Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0" *Mar 1

```
00:30:00.780: RADIUS: Calling-Station-Id [31] 16"0040.96af.3e93" *Mar 1 00:30:00.758:
RADIUS: 92 D4 24 49 04 C2 D2 0A C3 CE E9 00 6B F1 B2 AF [??$I????????k???] *Mar 1
00:30:00.759: RADIUS: EAP-Message [79] 39 *Mar 1 00:30:00.759: RADIUS: 02 17 00 25 11 01 00
18 05 98 8B BE 09 E9 45 E2 [??????????????E?] *Mar 1 00:30:00.759: RADIUS: 73 5D 33 1D F0 2F
DB 09 50 AF 38 9F F9 3B BD D4 [s]3??/??P?8??;??] *Mar 1 00:30:00.759: RADIUS: 75 73 65 72 31
[user1] ---------------------------------------- Lines Omitted-------------------------
*Mar 1 00:30:00.781: RADIUS: State [24] 50 RADIUS: NAS-IP-Address [4] 6 10.77.244.194 *Mar 1
00:30:00.783: RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 00:30:00.822: RADIUS: Received from
id 1645/67 10.77.244.194:1812, Access-Accept, len 214 *Mar 1 00:30:00.822: RADIUS:
authenticator 10 0C B6 EE 7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A ---------------------------
----------- Lines Omitted--------------------------- *Mar 1 00:30:00.823: RADIUS: 75 73 65
72 31 [user1] *Mar 1 00:30:00.823: RADIUS: Vendor, Cisco [26] 59 *Mar 1 00:30:00.823:
RADIUS: Cisco AVpair [1] 53 "leap:session-key=?+*ve=];q,oi[d6|-z." *Mar 1 00:30:00.823:
RADIUS: User-Name [1] 28 "user1 *Mar 1 00:30:00.824: RADIUS: Message-Authenticato[80] 18
*Mar 1 00:30:00.824: RADIUS: 06 2D BA 93 10 C0 91 F8 B4 B8 A4 00 82 0E 11 36 [?-
????????????6] *Mar 1 00:30:00.826: RADIUS/DECODE: EAP-Message fragments, 37, total 37
bytes *Mar 1 00:30:00.826: found leap session key *Mar 1 00:30:00.830: %DOT11-6-ASSOC:
Interface Dot11Radio0, Station Station Name Associated KEY_MGMT[NONE]
```

- **пакеты debug radius local-server** — Эта отладка показывает все процессы, сделанные и с точки зрения сервера RADIUS.

Дополнительные сведения

- Настройка точки доступа как локального устройства проверки подлинности
- Настройка типов аутентификации
- Настройка серверов RADIUS и TACACS+
- Cisco Systems – техническая поддержка и документация