EAP−FAST with the Internal RADIUS Server on the Autonomous Access Point Configuration Example

Document ID: 116580

Contributed by Surendra BG, Cisco TAC Engineer.
Oct 10, 2013

Contents

Introduction

This document describes how to configure the Autonomous Access Point to act as a RADIUS server that performs Cisco Extensible Authentication Protocol−Flexible Authentication via Secure Protocol (EAP−FAST) for client authenticatication with the latest Cisco IOS® release (15.2JB), which has been updated to have the look and feel of a GUI interface.

Usually an external RADIUS server is used in order to authenticate users. In some cases, this is not a feasible solution. In these situations, an access point (AP) can act as a RADIUS server. In this situation, users are authenticated against the local database configured in the access point. This is called a Local RADIUS Server feature. You can also make other access points in the network use the Local RADIUS Server feature on an AP.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt this configuration:

- Cisco IOS GUI or CLI
- Concepts behind Extensible Authentication Protocol (EAP)
- Service Set Identifier (SSID) configuration
- RADIUS

Components Used

The information in this document is based on a 3600 AP that runs Cisco IOS Release15.2JB and acts as an

internal RADIUS server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

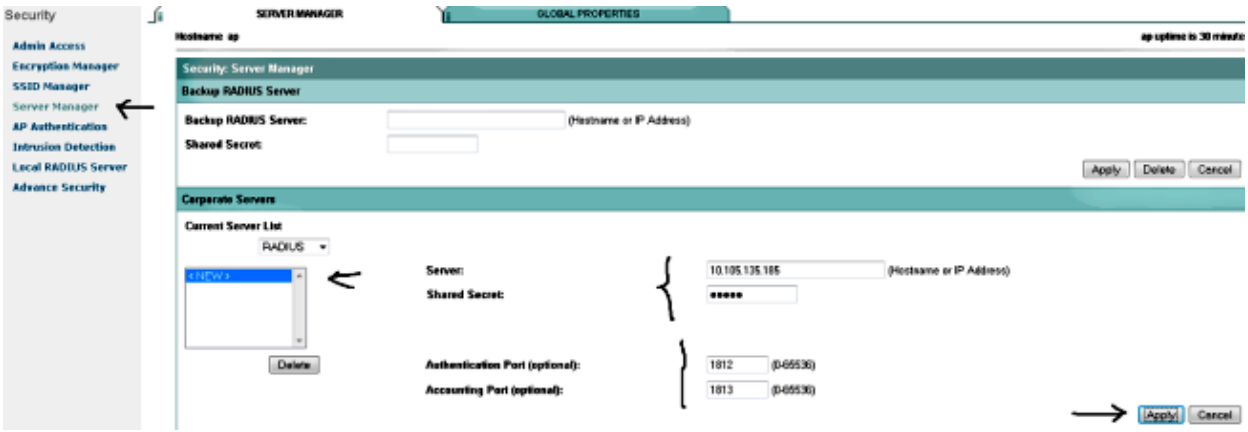
Configure

Configuration with GUI

1. In order to configure the AP as the Local RADIUS Server, navigate to ***AP GUI > Security > Server Manager***, and enter these details:
   - ***Hostname or IP Address***
   - ***Shared Secret***
   - ***Authentication Port***
   - ***Accounting Port***

   Note: For the Authentication and Accounting Ports, this example uses 1812 and 1813, respectively. However, 1645 and 1646 can also be used.

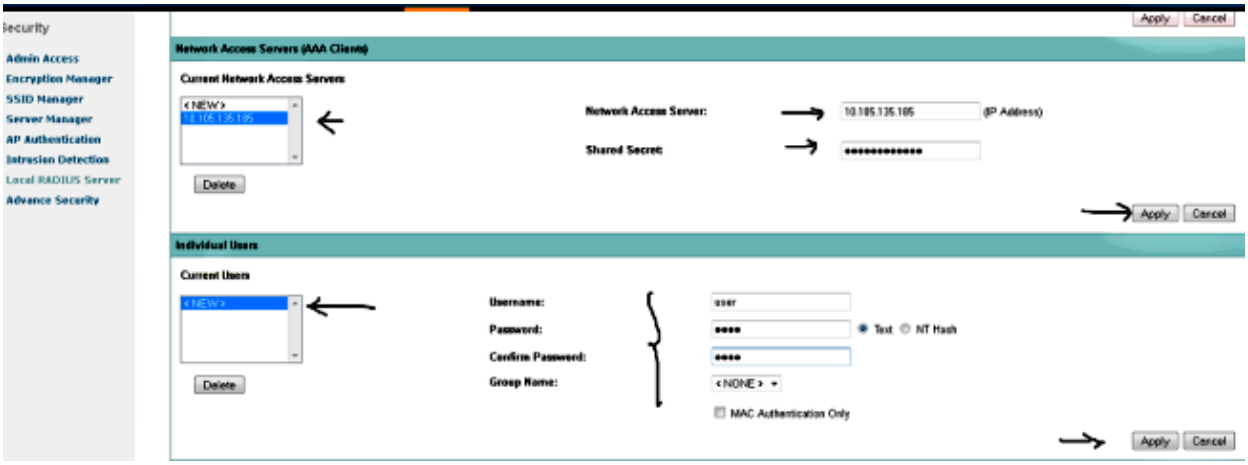
   Click ***Apply***.



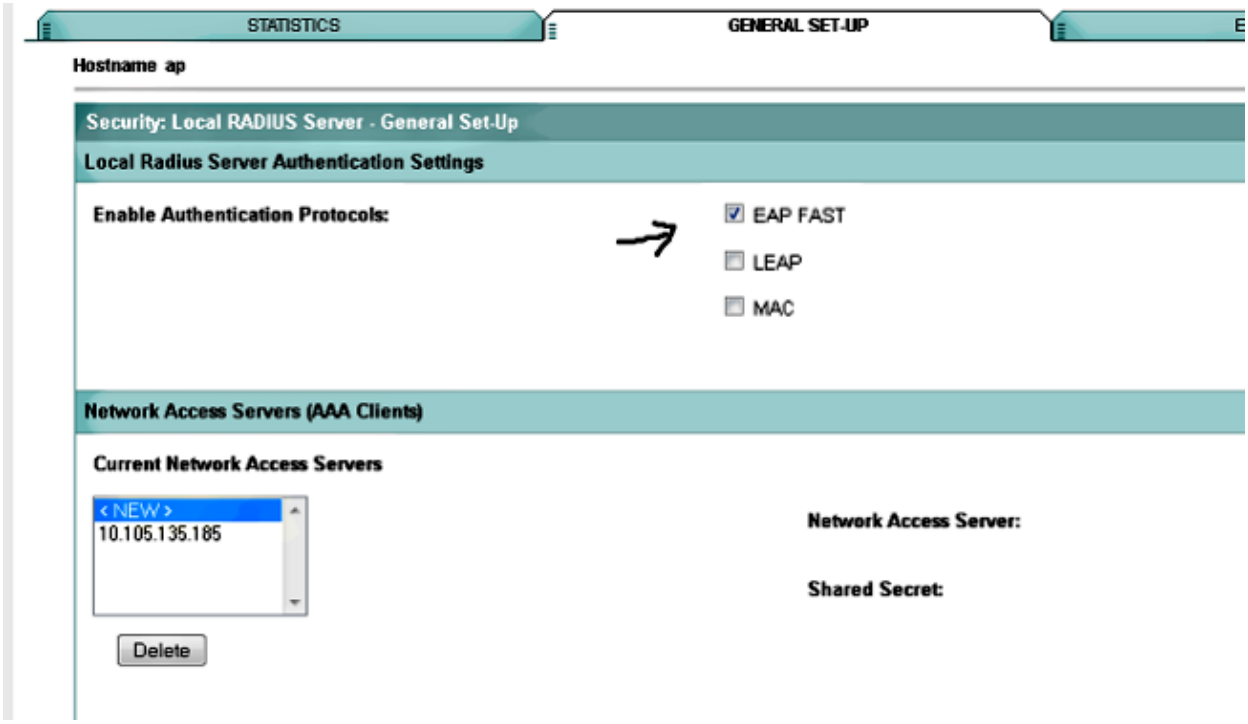
2. Navigate to the ***Local RADIUS Server*** configuration on the AP, click the ***General Set−Up*** tab, and enter these details:
   - ***Network Access Server*** (NAS) with the IP address of the AP (Bridge−Group Virtual Interface (BVI) int IP)
   - ***Shared Secret***

   Click ***Apply***.

   Create an ***Individual User*** with a ***Username*** and ***Password***. If a ***Group Name*** is required, then configure it (this example does not use a ***Group Name***).

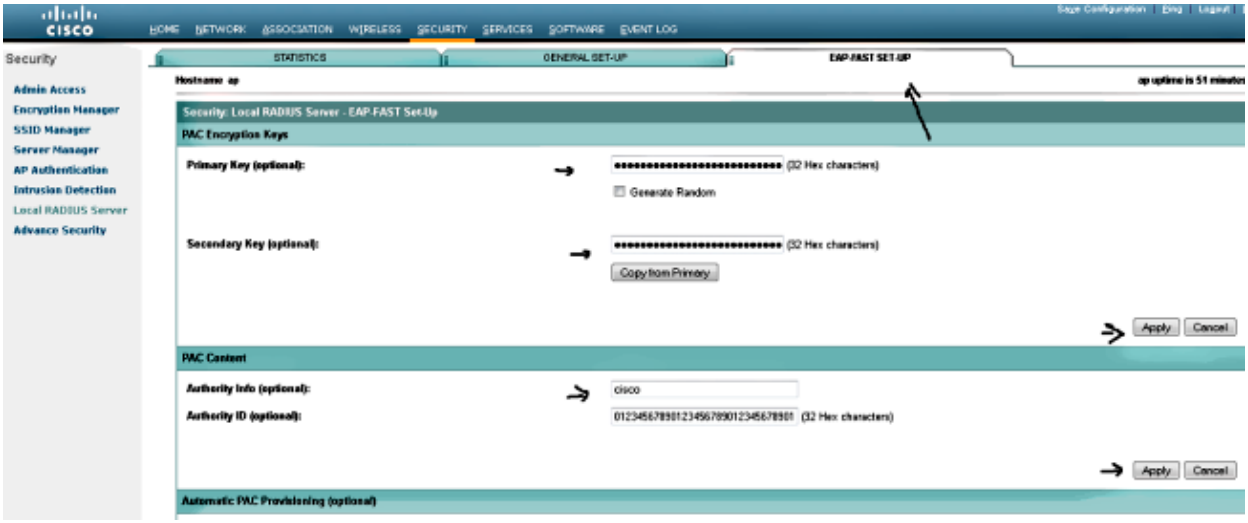


3. Uncheck the ***LEAP*** and ***MAC*** check boxes.

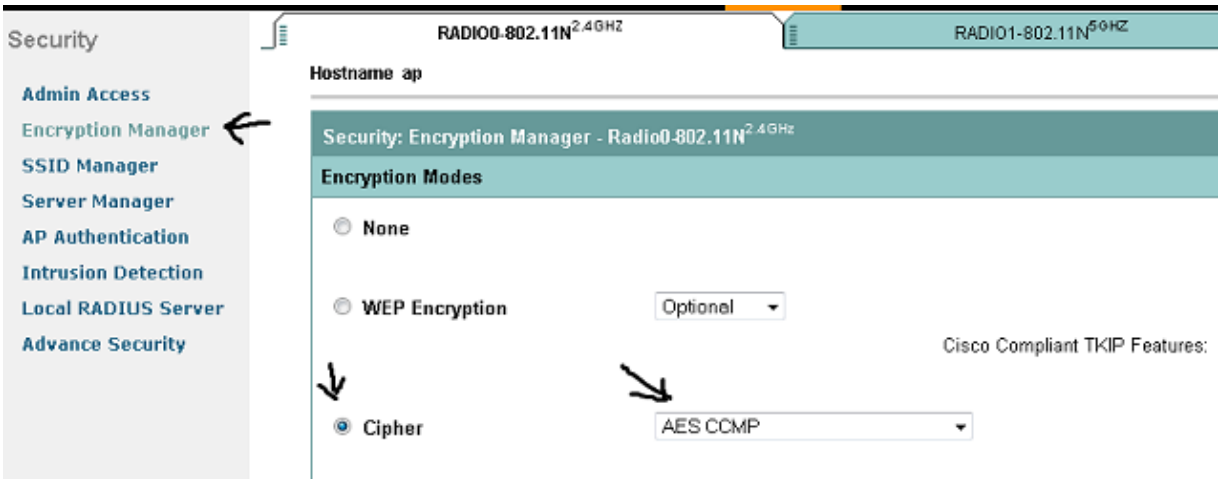


4. Click the ***EAP−FAST Set−Up*** tab, and enter the details for the ***PAC Encryption Keys*** and the ***PAC Content***.

Note: This example uses zero through nine four times since it has 32 Hex characters.

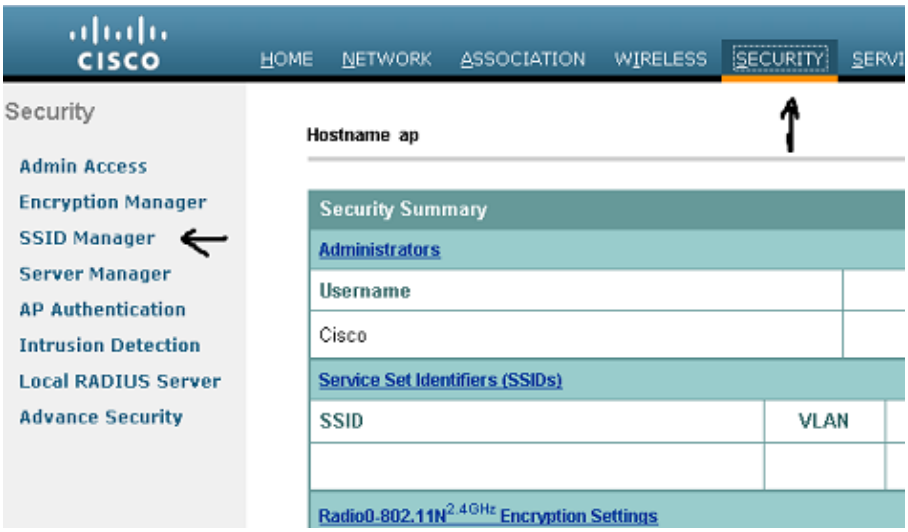


5. Navigate to the ***Encryption Manager***, configure ***Cipher*** with ***AES CCMP*** as the encryption, and click ***Apply All Radios*** or ***Required Radios***.

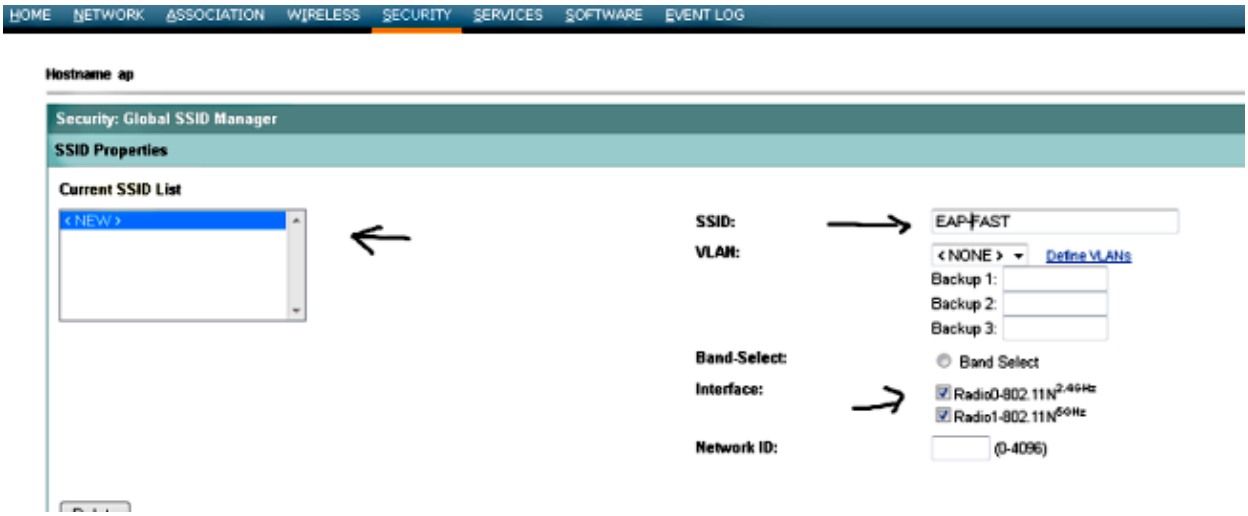


Configure the SSID

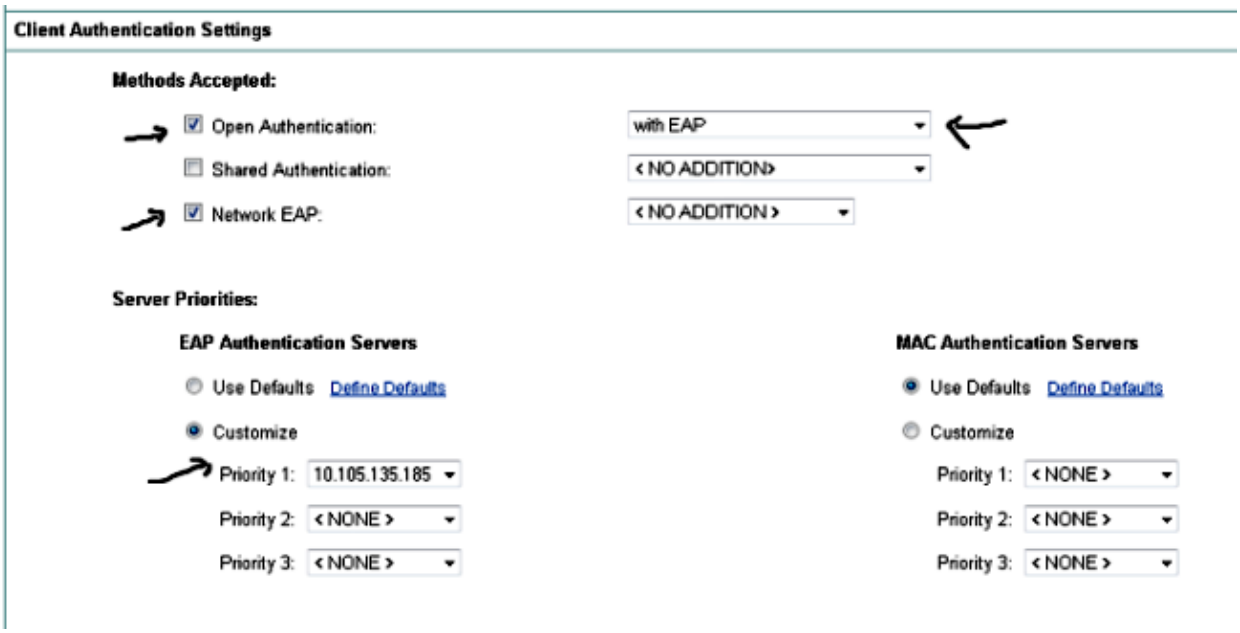
1. Navigate to ***Security*** > ***SSID manager***, and click ***Create New***.



2. Enter the details, and click ***Apply***.

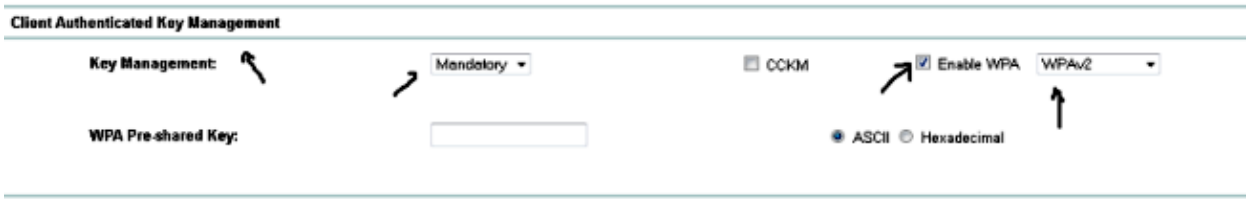


3. On the ***Client Authentication*** settings screen, check the ***Open Authentication*** check box, and select ***with EAP*** from the drop−down menu. Check the ***Network EAP*** check box, and select the ***RADIUS Server*** from the drop−down menu. This should be the AP IP address that you configured as AAA on the Server Manager and Local RADIUS Server page.

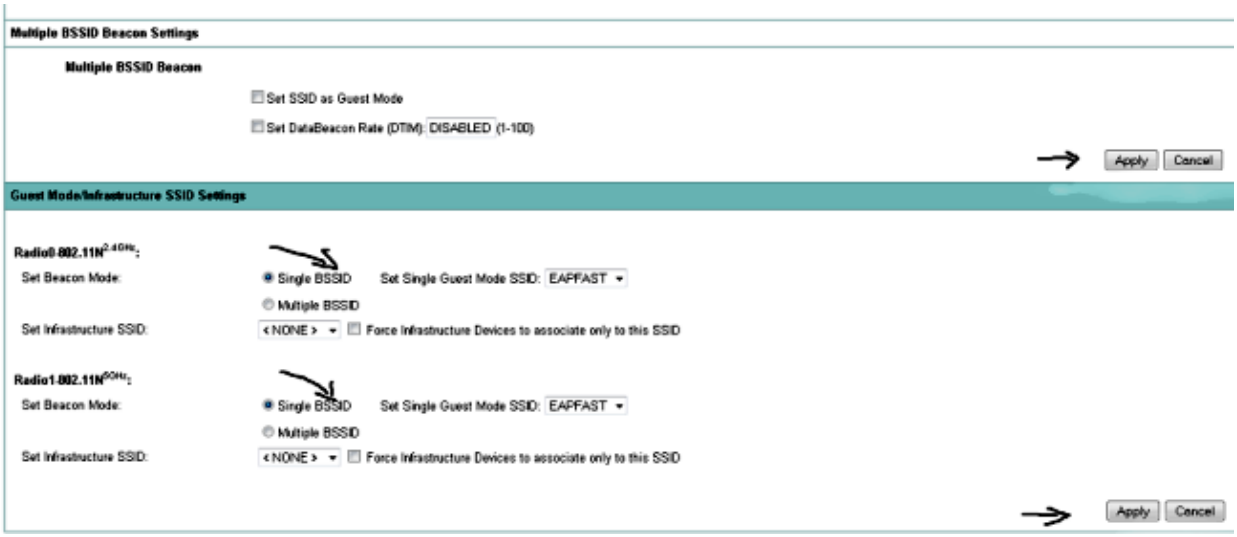


Configure Wireless Protected Access Version 2 (WPAv2) as Mandatory

1. On the ***Client Authenticated Key Management*** screen, select ***Mandatory*** from the ***Key Management*** drop−down menu. Check the ***Enable WPA*** check box, and select ***WPAv2*** from the drop−down menu.



2. Click ***Apply*** at the bottom of the page. In order to broadcast the SSID, click the ***Single SSID*** radio buttons, select the ***SSID*** from the drop−down menu, and click ***Apply***.



3. Navigate to ***Networks***, and enable the radios for ***2.4 GHz*** and ***5 GHz***. Ensure that the radios are up and running.

CLI Command for the Configurations

show run

```
Building configuration...

Current configuration : 3204 bytes
!
! Last configuration change at 01:11:36 UTC Mon Mar 1 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$06l4$E2pi.VeGTKUxxiwPScUEp.
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.105.135.185 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius rad_eap1
 server 10.105.135.185 auth-port 1812 acct-port 1813
```

```
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods1 group rad_eap1
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
dot11 syslog
!
dot11 ssid EAPFAST
   authentication open eap eap_methods1
   authentication network-eap eap_methods1
   authentication key-management wpa version 2
   guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 01300F175804
!
!
!
class-map match-all _class_voice0
 match ip dscp ef
 class-map match-all _class_voice1
 match ip dscp default
!
!
policy-map voice
 class _class_voice0
  set cos 6
 class _class_voice1
  set cos 6
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 stbc
 power local 14
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm
 !
 ssid EAPFAST
 !
 antenna gain 0
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address 10.105.135.185 255.255.255.128
 no ip route-cache
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
  eapfast authority id 01234567890123456789012345678901
  eapfast authority info cisco
  eapfast server-key primary 7 E1F54D861DC7150A7B949E5B4E630D8E5B
  eapfast server-key secondary 7 E7281DB670D36C052F60D36337436ABA13
  nas 10.105.135.185 key 7 01100F175804
  user user nthash 7 075A76681B514A2436465D28517D7A7178611403375334215677C79030
  D2D5448
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.105.135.185 auth-port 1812 acct-port 1813 key 7 045802150C2E
radius-server vsa send accounting
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
transport input all
!
end

ap#
```

Verify

If you connect to the client, then this is the log that displays on the AP after a successful authentication:

```
*Mar  1 00:45:02.035: %DOT11−4−UPLINK_ESTABLISHED: Interface Dot11Radio1,
Associated To AP root XXXX.XXXX.XXXX [EAP−FAST WPAv2]
```

Troubleshoot

Complete these steps in order to troubleshoot this configuration.

1. In order to eliminate the possibility that Radio Frequency (RF) issues prevent successful authentication, set the method on the SSID to ***Open*** in order to temporarily disable authentication.

2. From the GUI on the ***SSID Manager*** page, uncheck the ***Network−EAP*** check box, and check ***Open***.

3. From the CLI, use the commands ***authentication open*** and ***no authentication network−eap eap_methods***. If the client successfully associates, RF does not contribute to the association problem.

4. Verify that all shared secret passwords are synchronized. These lines must contain the same shared secret password:
   - radius−server host x.x.x.x auth−port x acct−port x key <*shared_secret*>
   - nas x.x.x.x key <*shared_secret*>
5. Remove any User Groups and their associated configurations. Sometimes conflicts occur between User Groups defined by the AP and User Groups on the domain.

Debug Commands

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

Here is a list of useful debug commands.

- ***debug dot11 aaa authenticator all*** − This debug shows the various negotiations that a client goes through as the client associates and authenticates through the 802.1x or EAP process from the perspective of the Authenticator (AP). This debug was introduced in Cisco IOS Software Release 12.2(15)JA. This command obsoletes ***debug dot11 aaa dot1x all*** in this and later releases.

```
 *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: 0x1101805F90: 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*** − This debug shows the RADIUS negotiations between the server and client, both of which, in this case, are the AP.

- ***debug radius local-server client*** − This debug shows the authentication of the client from the perspective of the RADIUS server.

```
*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 "EAP-FAST: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]
```

- ***debug radius local-server packets*** − This debug shows all of the processes that are executed by and from the perspective of the RADIUS server.