

# ワイヤレス LAN コントローラ ( WLC ) の Debug Client の説明

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[debug client](#)

[debug client のバリエーション](#)

[モビリティ](#)

[EAP 認証のトラブルシューティング](#)

[クライアント接続](#)

[コントローラ プロセス](#)

[Policy Enforcement Module \( PEM \)](#)

[クライアントトラフィック転送](#)

[Access Point Functions \( APF \)](#)

[802.1x 認証 \( Dot1x \)](#)

[debug client の分析](#)

[トラブルシューティングの例](#)

[誤ったクライアント暗号化設定](#)

[誤った事前共有キー](#)

[関連情報](#)

## 概要

このドキュメントでは、ワイヤレス LAN コントローラでの `debug client` コマンド出力について詳しく説明します。

このドキュメントでは、次のトピックを扱っています。

- ワイヤレス クライアントの処理方法
  - 関連付けと認証の基本的な問題のトラブルシューティング
- 分析する出力では、WPA 事前共有鍵 ( WPA-PSK ) ネットワークのシナリオを扱います。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ワイヤレス LAN コントローラ ( WLC ) と Lightweight アクセス ポイント ( LAP ) の基本動作のための設定方法
- Lightweight アクセス ポイント プロトコル ( LWAPP ) とワイヤレスのセキュリティ方式
- 802.11 認証プロセスと関連付けプロセスの動作方法

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ファームウェア 4.1 または 4.2 を実行する Cisco 2000/2100/4400 シリーズ WLC
- LWAPP ベースのアクセス ポイント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## debug client

コマンド **デバッグ クライアント** は <MACADDRESS> 提供される MAC アドレスのフィルタと 8 つの debug コマンドを、特定の MAC アドレスが示されている含まれているメッセージだけそう有効にするマクロです。8 個のデバッグ コマンドでは、クライアントの関連付けと認証について最も重要な詳細が表示されます。フィルタは、複数のワイヤレス クライアントがある状況で役立ちます。このような状況では、フィルタなしでデバッグを有効にすると、生成される出力が多すぎるか、コントローラが過負荷になります。

集まった情報では、クライアントの関連付けと認証について最も重要な詳細が扱われます ( 例外が 2 つあり、これについてはこのドキュメントの後半で説明します ) 。

有効になるコマンドは、次の出力のとおりです。

```
(Cisco Controller) >show debug MAC address ..... 00:00:00:00:00:00
Debug Flags Enabled: dhcp packet enabled. dot11 mobile enabled. dot11 state enabled. dot1x
events enabled. dot1x states enabled. pem events enabled. pem state enabled.
```

これらのコマンドでは、アドレス ネゴシエーション、802.11 クライアント ステート マシン、802.1x 認証、Policy Enforcement Module ( PEM )、アドレス ネゴシエーション ( DHCP ) が扱われます。

## debug client のバリエーション

ほとんどのシナリオに関しては、**デバッグ クライアント <MACAddress>** コマンドは情報を必要とされて得る十分です。ただし次のように、デバッグがさらに必要となる、2 つの重要な状況があります。

- [モビリティ](#) ( コントローラ間をローミングするクライアント )
- [EAP 認証のトラブルシューティング](#)

## [モビリティ](#)

コントローラ間のモビリティ プロトコル 相互対話のその他の情報を得るために **デバッグ クライアント <MACAddress >** コマンドがもたらされた後この場合、有効にされる **モビリティ デバッグ** 必要。

注: この出力の詳細については、別のドキュメントで今後扱います。

モビリティ デバッグを有効にするために、**デバッグ クライアント <MACAddress >** を使用し、次に **デバッグ モビリティ ハンドオフ enable** コマンドを使用して下さい:

```
(Cisco Controller) >debug client 00:00:00:00:00:00 (Cisco Controller) >debug mobility handoff enable (Cisco Controller) >show debug MAC address .....  
00:00:00:00:00:00 Debug Flags Enabled: dhcp packet enabled. dot11 mobile enabled. dot11 state enabled dot1x events enabled. dot1x states enabled. mobility handoff enabled. pem events enabled. pem state enabled.
```

## [EAP 認証のトラブルシューティング](#)

WLC と認証サーバ ( 外部 RADIUS または内部 EAP サーバ ) との間の相互対話をトラブルシューティングするには、コマンド **debug AAA all enable** を使用して必要な詳細を表示します。このコマンドは後 **デバッグ クライアント <MACAddress >** コマンドを使用する必要があった、その他の **デバッグ** コマンドで必要に応じて結合することができます (たとえば、**ハンドオフ**)。

```
(Cisco Controller) >debug client 00:00:00:00:00:00 (Cisco Controller) >debug aaa all enable (Cisco Controller) >show debug MAC address ..... 00:00:00:00:00:00  
Debug Flags Enabled: aaa detail enabled. aaa events enabled. aaa packet enabled. aaa packet enabled. aaa ldap enabled. aaa local-auth db enabled. aaa local-auth eap framework errors enabled. aaa local-auth eap framework events enabled. aaa local-auth eap framework packets enabled. aaa local-auth eap framework state machine enabled. aaa local-auth eap method errors enabled. aaa local-auth eap method events enabled. aaa local-auth eap method packets enabled. aaa local-auth eap method state machine enabled. aaa local-auth shim enabled. aaa tacacs enabled. dhcp packet enabled. dot11 mobile enabled. dot11 state enabled dot1x events enabled dot1x states enabled. mobility handoff enabled. pem events enabled. pem state enabled.
```

## [クライアント接続](#)

このドキュメントで使用する場合、**クライアント接続**とは、ワイヤレス クライアントが次の手順を実行するプロセスのことです。

### 802.11 セクション

1. 調査 : 関連付ける有効な AP を検索します。
2. 認証 : オープン (ヌル) または共有にすることができます。一般的にはオープンを選択します。
3. 関連付け : AP にデータ サービスを要求します。

### L2 ポリシー セクション

1. なし : 設定に応じて、PSK または EAP 認証が実行されます。

2. キー ネゴシエーション：暗号化方式を選択した場合。

## L3 ポリシー セクション

1. アドレス ラーニング。
2. Web 認証 ( 選択した場合 ) 。

注: これらの手順は、プロセス全体のサブセットまたは概要を表しています。このドキュメントでは単純にしたシナリオについて説明し、802.11 および L2 ポリシーを扱って、WPA-PSK およびアドレス ラーニングを使用します。外部 AAA または L3 ポリシーは認証用に使用しません。

## コントローラ プロセス

各セクションでは、コントローラが個別プロセスを使用して、それぞれの瞬間でのクライアントの状態を追跡します。プロセスはプロセス間で相互対話し、クライアントが接続テーブルに追加されることを確認します ( 設定されているセキュリティ ポリシーによる )。コントローラへのクライアント接続手順について理解するため、最も関連性のあるプロセスの概要を次に示します。

- **Policy Enforcement Module ( PEM )** : クライアントの状態を制御し、WLAN 設定のそれぞれのセキュリティ ポリシーでそれを強制します。
- **Access Point Functions ( APF )** : 基本的には802.11 ステート マシンです。
- **Dot1x** : ワイヤレス クライアントのために、802.1x、PSK 認証、キー処理のステート マシンを実装します。
- **モビリティ** : 同一モビリティ グループのその他のコントローラとの相互対話を追跡します。
- **Data Transformation Layer ( DTL )** : ソフトウェア コンポーネントとネットワーク ハードウェア アクセラレーション ( NPU ) との間に存在します。ARP 情報を制御します。

## Policy Enforcement Module ( PEM )

WLAN 設定に基づき、クライアントは一連の手順を実行します。PEM は、必要な L2 および L3 セキュリティ ポリシーに従うため、これが実行されていることを確認します。

クライアント デバッグの分析に関連する PEM ステートのサブセットを次に示します。

- **start** — New Client エントリのための最初のステータス。
- **AUTHCHECK** : 実施する L2 認証ポリシーが WLAN にあります。
- **8021X\_REQD** — クライアントは 802.1X 認証を完了する必要があります。
- **L2AUTHCOMPLETE** — クライアントは正常に L2 ポリシーを終えました。プロセスは L3 ポリシー ( アドレス ラーニング、Web 認証など ) に進むことができます。同一モビリティ グループのローミング クライアントの場合、コントローラはその他のコントローラから L3 情報を取得するために、ここでモビリティ アナウンスメントを送信します。
- **WEP\_REQD** — クライアントは WEP 認証を完了する必要があります。
- **DHCP\_REQD** — コントローラは、DHCP 要求 ARP要求によってされるクライアントからの L3 アドレスを学習する必要がありましたりまたはモビリティグループの他のコントローラから学ばれる情報によって、または更新します。必要な DHCP が WLAN でマークされている場合は、DHCP またはモビリティ情報のみが使用されます。
- **WEBAUTH\_REQD** — クライアントは Web 認証を完了する必要があります。 ( L3 ポリシー ) 。
- **RAN** — クライアントは正常に必須 L2 および L3 ポリシーを完了し、ネットワークに今トラフィックを送信できます。

次の図は単純な PEM ステート マシンを示しています。クライアントは RUN 状態になるまで遷移し、トラフィックをネットワークに送信できるようになります。



注: この図では、遷移と状態がすべて網羅されているわけではありません。分かりやすくするため、一部の中間ステップを削除してあります。

## クライアントトラフィック転送

START 状態から最後の RUN 状態の前まで、クライアントトラフィックはネットワークに転送されず、コントローラのメイン CPU に渡されて分析されます。転送される情報は、状態および実施されているポリシーによって決まります。たとえば 802.1x が有効である場合、EAPOL トラフィックは CPU に転送されます。Web 認証を使用する場合は、CPU が HTTP と DNS を許可してインターセプトし、Web リダイレクションを実行してクライアント認証クレデンシャルを取得するという例を挙げることもできます。

クライアントが RUN 状態に達すると、クライアント情報は NPU に送信されて FastPath スイッチングが有効になります。これによってユーザトラフィックはクライアント VLAN にケーブルレートで転送され、ユーザデータ転送タスクの中央の CPU は解放されます。

転送されるトラフィックは、NPU に適用されるクライアントタイプによって決まります。関連性の最も高いタイプについて、次の表で説明します。

タイプ	説明
1	通常のクライアントトラフィック転送。
9	IP ラーニング状態。このクライアントから CPU に 1 つのパケットが送信され、使用されている IP アドレスが取得されます。
2	ACL パススルー。NPU に通知するように ACL が WLAN で設定されているときに使用されます。

## Access Point Functions ( APF )

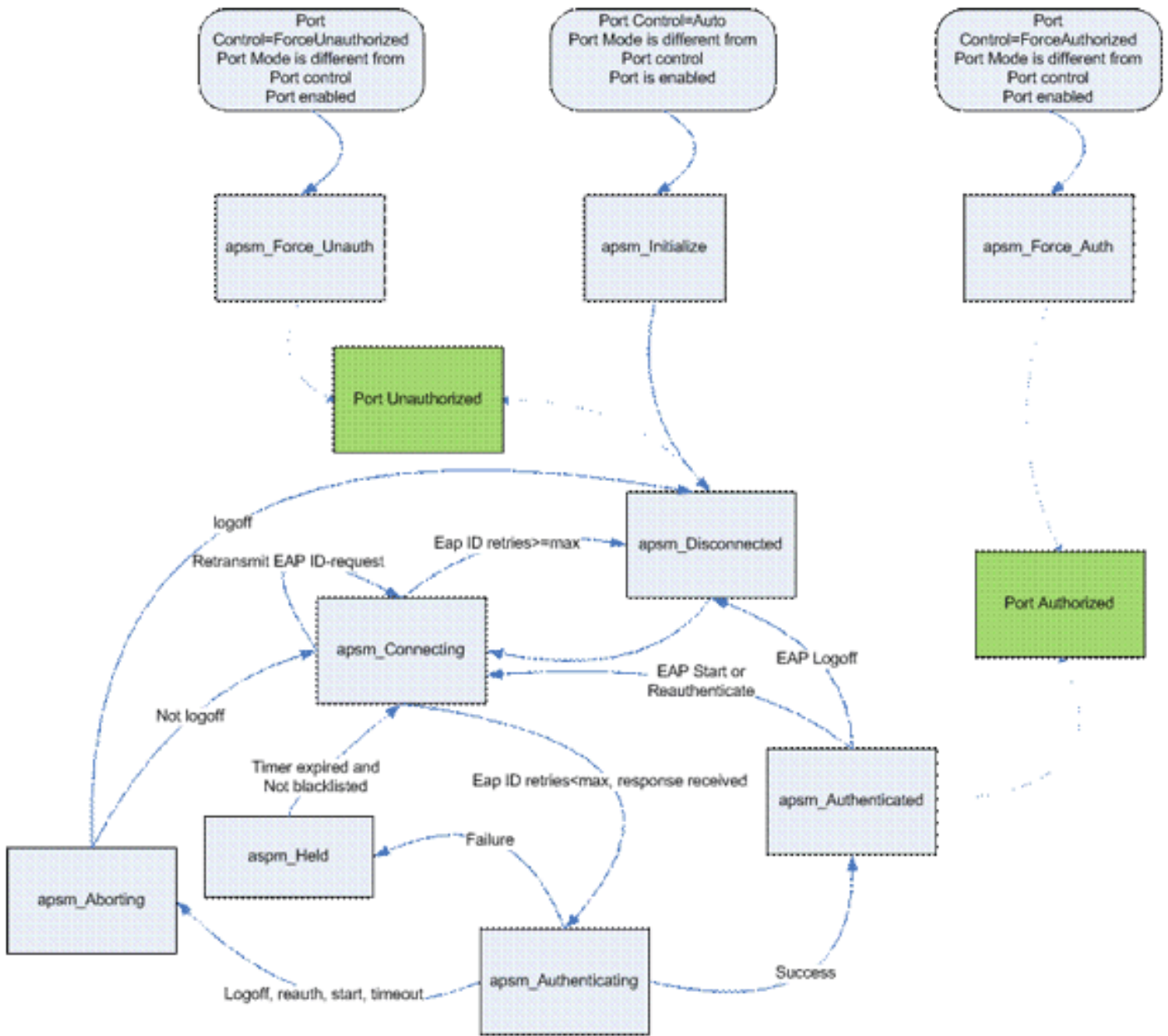
このプロセスでは 802.11 マシン ステートでクライアントの状態が処理され、さまざまなローミングシナリオを検証するためにモビリティコードとの相互対話が行われます。このドキュメントでは、モビリティの詳細またはその状態について説明しません。

次の表では、関連性の高いクライアント状態について説明します。コントローラへのクライアントの関連付け中に、このような状態になります。

名前	説明
アイドル	新規クライアント、または一部の状況の一時的な状態。
AAA Pending	クライアントは MAC アドレス認証を待機中。
Authenticated	オープン認証が正常に行われたか、一部の状況の中間的な状態。
Associated	クライアントは MAC 認証プロセスおよびオープン認証プロセスを正常に通過。
Disassociated	クライアントが関連付け解除/認証解除を送信したか、関連付けタイマーが期限切れ。
To Delete	クライアントを削除対象としてマーク ( 一般的には除外タイマーが期限切れになった後 ) 。
Probe	新しいクライアントのプロブ要求を受信。
Excluded/Blacklisted	クライアントを除外対象としてマーク。一般的には WPS ポリシーに関連。
Invalid	クライアント状態のエラー。

次の図はステートマシンの遷移を示していますが、関連性の最も高い状態および遷移のみを示しています。





## debug client の分析

```

APF Process Wed Oct 31 10:46:13 2007: 00:1b:77:42:07:69 Adding mobile on LWAPP AP
00:1c:0j:ca:5f:c0(0) !--- A new station is received. After validating type, it is added to the
!--- AP that received it. This can happen both on processing association !--- request or probe
requests Wed Oct 31 10:46:13 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station:
(callerId: 23) in 5 seconds !--- Sets an expiration timer for this entry in case it does not
progress !--- beyond probe status. 5 Seconds corresponds to Probe Timeout. This message !---
might appear with other time values since, during client processing, !--- other functions might
set different timeouts depending on state. Wed Oct 31 10:46:13 2007: 00:1b:77:42:07:69
apfProcessProbeReq (apf_80211.c:4057) Changing state for mobile 00:1b:77:42:07:69 on AP
00:1c:0j:ca:5f:c0 from Idle to Probe !--- APF state machine is updated. Wed Oct 31 10:46:13
2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds !---
New Probe request update sent AP about client. IMPORTANT: !--- Access points do not forward all
probe requests to the controller; they !--- summarize per time interval (by default 500 msec).
This information is !--- used later by location and load balancing processes. Wed Oct 31
10:46:14 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 24) in 5
seconds !--- New Probe request update sent AP about client. Wed Oct 31 10:46:14 2007:
00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds !--- New
Probe request update sent AP about client. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69
Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds !--- New Probe request update

```



sent AP about client. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Association received from mobile on AP 00:1c:0j:ca:5f:c0 !--- Access point reports an association request from the client. !--- When the process reaches this point, the client is not excluded and not !--- in mobility intermediate state Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 STA - rates (8): 140 18 152 36 176 72 96 108 0 0 0 0 0 0 0 0 !--- Controller saves the client supported rates into its connection table. !--- Units are values of 500 kbps, basic (mandatory) rates have the Most Significant bit (MSb) set. !--- The above would be 6mbps basic, 9, 12 basic, 18, 24 basic, 36, 48, 54 Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Processing WPA IE type 221, length 24 for mobile 00:1b:77:42:07:69 !--- Controller validates the 802.11i security information element. **PEM Process** Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0 START (0) Deleted mobile LWAPP rule on AP [00:1c:0j:ca:5f:c0] !--- As the client requests new association, APF requests to PEM to delete the !--- client state and remove any traffic forwarding rules that it could have. **APF Process** Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Updated location for station old AP 00:00:00:00:00:00-0, new AP 00:1c:0j:ca:5f:c0-1 !--- APF updates where this client is located. For example, this client is !--- a new addition; therefore, no value exists for the old location. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0 START (0) Initializing policy !--- PEM notifies that this is a new user. Security policies are checked !--- for enforcement. **PEM Process** Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state AUTHCHECK (2) !--- PEM marks as authentication check needed. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0 AUTHCHECK (2) Change state to 8021X\_REQD (3) last state 8021X\_REQD !--- After the WLAN configuration is checked, the client will need either !--- 802.1x or PSK authentication Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0 8021X\_REQD (3) Plumbed mobile LWAPP rule on AP 00:1c:0j:ca:5f:c0 !--- PEM notifies the LWAPP component to add the new client on the AP with !--- a list of negotiated capabilities, rates, Qos, etc. **APF Process** Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 apfPemAddUser2 (apf\_policy.c:209) Changing state for mobile 00:1b:77:42:07:69 on AP 00:1c:0j:ca:5f:c0 from Probe to Associated !--- APF notifies that client has been moved successfully into associated !--- state. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Stopping deletion of Mobile Station: (callerId: 48) !--- The expiration timer for client is removed, as now the session timeout !--- is taking place. This is also part of the above notification !--- (internal code callerId: 48). Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Sending Assoc Response to station on BSSID 00:1c:0j:ca:5f:c0 (status 0) !--- APF builds and sends the association response to client. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 apfProcessAssocReq (apf\_80211.c:3838) Changing state for mobile 00:1b:77:42:07:69 on AP 00:1c:0j:ca:5f:c0 from Associated to Associated !--- The association response was sent successfully; now APF keeps the !--- client in associated state and sets the association timestamp on this point. **Dot1x Process** Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Creating a new PMK Cache Entry for station 00:1b:77:42:07:69 (RSN 0) !--- APF calls Dot1x to allocate a new PMK cached entry for the client. !--- RSN is disabled (zero value). Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Initiating WPA PSK to mobile 00:1b:77:42:07:69 !--- Dot1x signals a new WPA or WPA2 PSK exchange with mobile. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 dot1x - moving mobile 00:1b:77:42:07:69 into Force Auth state !--- As no EAPOL authentication takes place, the client port is marked as !--- forced Auth. Dot1x performs key negotiation with PSK clients only. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Skipping EAP-Success to mobile 00:1b:77:42:07:69 !--- For PSK, CCKM or RSN, the EAP success is not sent to client, as there !--- was no EAPOL authentication taking place. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Sending EAPOL-Key Message to mobile 00:1b:77:42:07:69 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 !--- Dot1x starts the exchange to arrive into PTK. PMK is known, as this !--- is PSK auth. First message is ANonce. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Received EAPOL-Key from mobile 00:1b:77:42:07:69 !--- Message received from client. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Received EAPOL-key in PKT\_START state (message 2) from mobile 00:1b:77:42:07:69 !--- This signals the start of the validation of the second message !--- from client (SNonce+MIC). No errors are shown, so process continues. !--- Potential errors at this point could be: deflection attack (ACK bit !--- not set on key), MIC errors, invalid key type, invalid key length, etc. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Stopping retransmission timer for mobile 00:1b:77:42:07:69 !--- Dot1x got an answer for message 1, so retransmission timeout is stopped. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Sending EAPOL-Key Message to mobile 00:1b:77:42:07:69 state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01 !--- Derive PTK; send GTK + MIC. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Received EAPOL-Key from mobile 00:1b:77:42:07:69 !--- Message received from client. Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 Received EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile 00:1b:77:42:07:69 !--- This signals the start of validation of message 4 (MIC), which !--- means client installed the keys. Potential errors after this message !--- are MIC validation errors, invalid key types, etc. **PEM Process** Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0 8021X\_REQD (3) Change state to L2AUTHCOMPLETE (4) last state

L2AUTHCOMPLETE (4) *!--- PEM receives notification and signals the state machine to change to L2 !--- authentication completed.* Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0

L2AUTHCOMPLETE (4) *Plumbed mobile LWAPP rule on AP 00:1c:0j:ca:5f:c0 !--- PEM pushes client status and keys to AP through LWAPP component.* Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0

L2AUTHCOMPLETE (4) *Change state to DHCP\_REQD (7) last state DHCP\_REQD (7) !--- PEM sets the client on address learning status.* Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *pemAdvanceState2 4238, Adding TMP rule !--- PEM signals NPU to allow DHCP/ARP traffic to be inspected by controller !--- for the address learning.* Wed Oct 31 10:46:15 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *Adding Fast Path rule type = Airespace AP - Learn IP address on AP 00:1c:0j:ca:5f:c0, slot 1, interface = 1, QOS = 0 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006 !--- Entry is built for client and prepared to be forwarded to NPU. !--- Type is 9 (see the table in the [Client Traffic Forwarding](#) section of !--- this document) to allow controller to learn the IP address.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *Successfully plumbed mobile rule (ACL ID 255) !--- A new rule is successfully sent to internal queue to add the client !--- to the NPU. **Dot1x Process*** Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Stopping retransmission timer for mobile* 00:1b:77:42:07:69

*!--- Dot1x received message from client.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Sending EAPOL-Key Message to mobile 00:1b:77:42:07:69 state PTKINITDONE (message 5 - group), replay counter 00.00.00.00.00.00.02 !--- Group key update prepared for client. **PEM Process*** Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

*Added NPU entry of type 9 !--- NPU reports that entry of type 9 is added (learning address state). !--- See the table in the [Client Traffic Forwarding](#) section of this document.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Sent an XID frame !--- No address known yet, so the controller sends only XID frame !--- (destination broadcast, source client address, control 0xAF). **Dot1x Process*** Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Sent EAPOL-Key M5 for mobile 00:1b:77:42:07:69 !--- Key update sent.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Received EAPOL-Key from mobile 00:1b:77:42:07:69 !--- Key received.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Received EAPOL-key in REKEYNEGOTIATING state (message 6) from mobile 00:1b:77:42:07:69 !--- Successfully received group key update.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Stopping retransmission timer for mobile 00:1b:77:42:07:69 !--- Group key timeout is removed. **DHCP Process*** Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*DHCP received op BOOTREQUEST (1) (len 308, port 1, encap 0xec03) !--- First DHCP message received from client.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*DHCP dropping packet due to ongoing mobility handshake exchange, (siaddr 0.0.0.0, mobility state = 'apfMsMmQueryRequested' **PEM Process*** Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*0.0.0.0 DHCP\_REQD (7) mobility role update request from Unassociated to Local Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 192.168.100.11 !--- NPU is notified that this controller is the local anchor, so to !--- terminate any previous mobility tunnel. As this is a new client, !--- old address is empty.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *State Update from Mobility-Incomplete to Mobility-Complete, mobility role=Local !--- Role change was successful.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *pemAdvanceState2 3934, Adding TMP rule !--- Adding temporary rule to NPU for address learning now with new mobility !--- role as local controller.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *Replacing Fast Path rule type = Airespace AP - Learn IP address on AP 00:1c:0j:ca:5f:c0, slot 1, interface = 1, QOS = 0 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006 !--- Entry is built.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

DHCP\_REQD (7) *Successfully plumbed mobile rule (ACL ID 255) !--- A new rule is successfully sent to internal queue to add the !--- client to the NPU.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69 0.0.0.0

*Added NPU entry of type 9 !--- Client is on address learning state; see the table in the !--- [Client Traffic Forwarding](#) section of this document. Now mobility !--- has finished.* Wed Oct 31 10:46:19 2007: 00:1b:77:42:07:69

*Sent an XID frame !--- No address known yet, so controller sends only XID frame (destination !--- broadcast, source client address, control 0xAF). **DHCP Process*** Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP received op BOOTREQUEST (1) (len 308, port 1, encap 0xec03) !--- DHCP request from client.* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP selecting relay 1 - control block settings: dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0 !--- Based on the WLAN configuration, the controller selects the identity to !--- use to relay the DHCP messages.* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP selected relay 1 - 192.168.100.254 (local address 192.168.100.11, gateway 192.168.100.254, VLAN 100, port 1) !--- Interface selected.* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP transmitting DHCP DISCOVER (1)* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP xid: 0xd3d3b6e9 (3553867497), secs: 1024, flags: 0* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP chaddr: 00:1b:77:42:07:69* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0* Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69

*DHCP siaddr: 0.0.0.0, giaddr: 192.168.100.11 !--- Debug parsing of the frame*

sent. The most important fields are included. Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP sending REQUEST to 192.168.100.254 (len 350, port 1, vlan 100) !--- DHCP request forwarded. Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP selecting relay 2 - control block settings: dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 192.168.100.11 VLAN: 100 Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP selected relay 2 ? NONE !--- No secondary server configured, so no additional DHCP request are !--- prepared (configuration dependant). Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00) Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP setting server from OFFER (server 192.168.100.254, yiaddr 192.168.100.105) !--- DHCP received for a known server. Controller discards any offer not on !--- the DHCP server list for the WLAN/Interface. Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP sending REPLY to STA (len 416, port 1, vlan 100) !--- After building the DHCP reply for client, it is sent to AP for forwarding. Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP transmitting DHCP OFFER (2) Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP xid: 0xd3d3b6e9 (3553867497), secs: 0, flags: 0 Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP chaddr: 00:1b:77:42:07:69 Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.100.105 Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP server id: 1.1.1.1 rcvd server id: 192.168.100.254 !--- Debug parsing of the frame sent. The most important fields are included. Wed Oct 31 10:46:21 2007: 00:1b:77:42:07:69 DHCP received op BOOTREQUEST (1) (len 316, port 1, encap 0xec03) !--- Client answers Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP selecting relay 1 - control block settings: dhcpServer: 192.168.100.254, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 192.168.100.11 VLAN: 100 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP selected relay 1 - 192.168.100.254 (local address 192.168.100.11, gateway 192.168.100.254, VLAN 100, port 1) !--- DHCP relay selected per WLAN config Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP transmitting DHCP REQUEST (3) Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP xid: 0xd3d3b6e9 (3553867497), secs: 1024, flags: 0 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP chaddr: 00:1b:77:42:07:69 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP siaddr: 0.0.0.0, giaddr: 192.168.100.11 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP requested ip: 192.168.100.105 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP server id: 192.168.100.254 rcvd server id: 1.1.1.1 !--- Debug parsing of the frame sent. The most important fields are included. Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP sending REQUEST to 192.168.100.254 (len 358, port 1, vlan 100) !--- Request sent to server. Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP selecting relay 2 - control block settings: dhcpServer: 192.168.100.254, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 192.168.100.11 VLAN: 100 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP selected relay 2 ? NONE !--- No other DHCP server configured. Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00) !--- Server sends a DHCP reply, most probably an ACK (see below). **PEM Process** Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 192.168.100.105 DHCP\_REQD (7) Change state to RUN (20) last state RUN (20) !--- DHCP negotiation successful, address is now known, and client !--- is moved to RUN status. Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 192.168.100.105 RUN (20) Reached PLUMBFASTPATH: from line 4699 !--- No L3 security; client entry is sent to NPU. Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 192.168.100.105 RUN (20) Replacing Fast Path rule type = Airespace AP Client on AP 00:1c:0j:ca:5f:c0, slot 1, interface = 1, QOS = 0 ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 192.168.100.105 RUN (20) Successfully plumbed mobile rule (ACL ID 255) **DHCP Process** Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 Assigning Address 192.168.100.105 to mobile Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP sending REPLY to STA (len 416, port 1, vlan 100) Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP transmitting DHCP ACK (5) Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP xid: 0xd3d3b6e9 (3553867497), secs: 0, flags: 0 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP chaddr: 00:1b:77:42:07:69 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.100.105 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 DHCP server id: 1.1.1.1 rcvd server id: 192.168.100.254 **PEM Process** Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 192.168.100.105 Added NPU entry of type 1 !--- Client is now successfully associated to controller. !--- Type is 1; see the table in the [Client Traffic Forwarding](#) !--- section of this document. Wed Oct 31 10:46:25 2007: 00:1b:77:42:07:69 Sending a gratuitous ARP for 192.168.100.105, VLAN Id 100 !--- As address is known, gratuitous ARP is sent to notify.

## トラブルシューティングの例

## 誤ったクライアント暗号化設定

この例では、AP に対する機能が異なるクライアントを示します。クライアントは SSID を調査していますが、プローブ要求はサポートされていないパラメータを示すため、クライアントは認証/関連付けフェーズに進むことができません。特にここで紹介する問題は、WPA を使用するクライアントと WPA2 サポートのみをアドバタイズする AP との間の不一致です。

```
Wed Oct 31 10:51:37 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 23) in 5 seconds
Wed Oct 31 10:51:37 2007: 00:1b:77:42:07:69 apfProcessProbeReq
(apf_80211.c:4057) Changing state for mobile 00:1b:77:42:07:69 on AP
00:1c:b0:ea:5f:c0 from Idle to Probe
!--- Controller adds the new client, moving into probing status Wed Oct 31 10:51:37 2007:
00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 24) in 5 seconds Wed Oct 31
10:51:38 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 24) in 5
seconds Wed Oct 31 10:51:38 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station:
(callerId: 24) in 5 seconds !--- AP is reporting probe activity every 500 ms as configured

Wed Oct 31 10:51:41 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:41 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:41 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:41 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:44 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:44 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:44 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:44 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:51:49 2007: 00:1b:77:42:07:69 apfMsExpireCallback (apf_ms.c:433)
Expiring Mobile!
Wed Oct 31 10:51:49 2007: 00:1b:77:42:07:69 0.0.0.0 START (0) Deleted mobile
LWAPP rule on AP [00:1c:b0:ea:5f:c0]
Wed Oct 31 10:51:49 2007: 00:1b:77:42:07:69 Deleting mobile on AP
00:1c:b0:ea:5f:c0(0)
!--- After 5 seconds of inactivity, client is deleted, never moved into !--- authentication or
association phases.
```

## 誤った事前共有キー

ここでは、クライアントがインフラストラクチャに WPA-PSK で認証しようとしていますが、クライアントとコントローラの間で事前共有キーが一致しないためにエラーになり、最終的にクライアントがブラックリスト登録されます。

```
Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Adding mobile on LWAPP AP
00:1c:b0:ea:5f:c0(0)
Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 23) in 5 seconds
Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 apfProcessProbeReq (apf_80211.c:
4057) Changing state for mobile 00:1b:77:42:07:69 on AP 00:1c:b0:ea:5f:c0
from Idle to Probe
Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile
Station: (callerId: 24) in 5 seconds
Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Association received from mobile
on AP 00:1c:b0:ea:5f:c0
```

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 STA - rates (8): 130 132 139 150  
12 18 24 36 0 0 0 0 0 0 0

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 STA - rates (12): 130 132 139 150  
12 18 24 36 48 72 96 108 0 0 0 0

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Processing WPA IE type 221,  
length 24 for mobile 00:1b:77:42:07:69

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 0.0.0.0 START (0)  
Initializing policy

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 0.0.0.0 START (0) Change state to  
AUTHCHECK (2) last state AUTHCHECK (2)

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 0.0.0.0 AUTHCHECK (2) Change  
state to 8021X\_REQD (3) last state 8021X\_REQD (3)

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 0.0.0.0 8021X\_REQD (3) Plumbed  
mobile LWAPP rule on AP 00:1c:b0:ea:5f:c0

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 apfPemAddUser2 (apf\_policy.c:209)  
Changing state for mobile 00:1b:77:42:07:69 on AP 00:1c:b0:ea:5f:c0 from  
Probe to Associated

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Stopping deletion of Mobile  
Station: (callerId: 48)

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Sending Assoc Response to station  
on BSSID 00:1c:b0:ea:5f:c0 (status 0)

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 apfProcessAssocReq (apf\_80211.c:  
3838) Changing state for mobile 00:1b:77:42:07:69 on AP 00:1c:b0:ea:5f:c0  
from Associated to Associated

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Creating a new PMK Cache Entry  
for station 00:1b:77:42:07:69 (RSN 0)

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Initiating WPA PSK to mobile  
00:1b:77:42:07:69

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 dot1x - moving mobile  
00:1b:77:42:07:69 into Force Auth state

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Skipping EAP-Success to mobile  
00:1b:77:42:07:69

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Sending EAPOL-Key Message to  
mobile 00:1b:77:42:07:69  
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Received EAPOL-Key from mobile  
00:1b:77:42:07:69

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Received EAPOL-key in PKT\_START  
state (message 2) from mobile 00:1b:77:42:07:69

Wed Oct 31 10:55:55 2007: 00:1b:77:42:07:69 Received EAPOL-key M2 with  
invalid MIC from mobile 00:1b:77:42:07:69

Wed Oct 31 10:55:56 2007: 00:1b:77:42:07:69 802.1x 'timeoutEvt' Timer expired  
for station 00:1b:77:42:07:69

Wed Oct 31 10:55:56 2007: 00:1b:77:42:07:69 Retransmit 1 of EAPOL-Key M1  
(length 99) for mobile 00:1b:77:42:07:69

Wed Oct 31 10:55:56 2007: 00:1b:77:42:07:69 Received EAPOL-Key from mobile  
00:1b:77:42:07:69

Wed Oct 31 10:55:56 2007: 00:1b:77:42:07:69 Received EAPOL-key in PKT\_START  
state (message 2) from mobile 00:1b:77:42:07:69

Wed Oct 31 10:55:56 2007: 00:1b:77:42:07:69 Received EAPOL-key M2 with invalid  
MIC from mobile 00:1b:77:42:07:69

*!--- MIC error due to wrong preshared key* Wed Oct 31 10:55:57 2007: 00:1b:77:42:07:69 802.1x  
'timeoutEvt' Timer expired for station 00:1b:77:42:07:69 Wed Oct 31 10:55:57 2007:  
00:1b:77:42:07:69 Retransmit 2 of EAPOL-Key M1 (length 99) for mobile 00:1b:77:42:07:69 Wed Oct  
31 10:55:57 2007: 00:1b:77:42:07:69 Received EAPOL-Key from mobile 00:1b:77:42:07:69 Wed Oct 31  
10:55:57 2007: 00:1b:77:42:07:69 Received EAPOL-key in PKT\_START state (message 2) from mobile  
00:1b:77:42:07:69 Wed Oct 31 10:55:57 2007: 00:1b:77:42:07:69 Received EAPOL-key M2 with invalid  
MIC from mobile 00:1b:77:42:07:69 Wed Oct 31 10:55:58 2007: 00:1b:77:42:07:69 802.1x  
'timeoutEvt' Timer expired for station 00:1b:77:42:07:69 Wed Oct 31 10:55:58 2007:  
00:1b:77:42:07:69 Retransmit failure for EAPOL-Key M1 to mobile 00:1b:77:42:07:69, retransmit  
count 3, mscb deauth count 0 Wed Oct 31 10:55:58 2007: 00:1b:77:42:07:69 Sent Deauthenticate to  
mobile on BSSID 00:1c:b0:ea:5f:c0 slot 0(caller 1x\_ptsm.c:462) *!--- Client is deauthenticated,  
after three retries !--- The process is repeated three times, until client is blacklisted* Wed  
Oct 31 10:56:10 2007: 00:1b:77:42:07:69 Blacklisting (if enabled) mobile 00:1b:77:42:07:69 Wed

Oct 31 10:56:10 2007: 00:1b:77:42:07:69 apfBlacklistMobileStationEntry2 (apf\_ms.c:3560) Changing state for mobile 00:1b:77:42:07:69 on AP 00:1c:b0:ea:5f:c0 from Associated to Exclusion-list (1)  
Wed Oct 31 10:56:10 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 44) in 10 seconds  
Wed Oct 31 10:56:10 2007: 00:1b:77:42:07:69 0.0.0.0 8021X\_REQD (3) Change state to START (0) last state 8021X\_REQD (3)  
Wed Oct 31 10:56:10 2007: 00:1b:77:42:07:69 0.0.0.0 START (0) Reached FAILURE: from line 3522  
Wed Oct 31 10:56:10 2007: 00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 9) in 10 seconds

## [関連情報](#)

- [Lightweight アクセス ポイントに関する FAQ \( 英語 \)](#)
- [ワイヤレス LAN コントローラ \( WLC \) に関する FAQ](#)
- [Cisco ワイヤレス LAN コントローラ モジュールに関する Q&A](#)
- [Wireless LAN Controller \( WLC \) に関する FAQ](#)
- [Unified Wireless Network における Radio Resource Management \( RRM \)](#)
- [ワイヤレス LAN \( WLAN \) 技術に関するサポート](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)