Entender o cliente de depuração em controladoras Wireless LAN (WLCs)

Contents

Introdução

Este documento descreve informações detalhadas sobre o **debug client** saída do comando em controladoras Wireless LAN (WLC).

Pré-requisitos

Requisitos

Este documento aborda estes tópicos:

- Como um cliente sem fio é tratado
- Como solucionar problemas básicos de associação e autenticação

A saída a ser analisada abrange o cenário para uma rede WPA-PSK (chave pré-compartilhada).

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar o WLC e o Lightweight Access Point (LAP) para a operação básica
- Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio
- Como os processos de autenticação e associação do 802.11 funcionam

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLCs Cisco AireOS (8540, 5520, vWLC) que executam o firmware 8.5 ou 8.10.
- Pontos de acesso baseados em CAPWAP.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Depurar cliente

O comando **debug client**
 é uma macro que ativa oito comandos de depuração, mais um filtro no endereço MAC fornecido, para que somente as mensagens que contêm o endereço MAC especificado sejam exibidas. Os oito comandos debug mostram os detalhes mais importantes sobre a associação e a autenticação de clientes. O filtro ajuda nas situações em que há vários clientes sem fio. Situações como quando muita saída é gerada ou o controlador é sobrecarregado quando a depuração é habilitada sem o filtro.

As informações coletadas abrangem detalhes importantes sobre a associação e a autenticação do cliente (com duas exceções mencionadas mais adiante neste documento).

Os comandos ativados são mostrados nesta saída:

```
<#root>

(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.
```

Esses comandos abrangem a negociação de endereço, a máquina de estado do cliente 802.11, a autenticação 802.1x, o Policy Enforcement Module (PEM) e a negociação de endereço (DHCP).

Depurar Variações de Cliente

Para a maioria dos cenários, o **debug client** é suficiente para obter as informações necessárias. No entanto, há duas situações importantes em que é necessária uma depuração adicional:

- Mobilidade (roaming de clientes entre controladores)
- Identificar e Solucionar Problemas de Autenticação EAP

Mobilidade

Nessa situação, as depurações de mobilidade precisam ser habilitadas após o comando **debug client** foi introduzido para obter informações adicionais sobre a interação do protocolo de mobilidade entre controladores.

> **Observação**: os detalhes dessa saída são abordados em outros documentos.

Para habilitar depurações de mobilidade, use o comando **debug client** e, em seguida, use o comando **debug mobility handoff enable** comando:

<#root>

```
(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.
```

Identificar e Solucionar Problemas de Autenticação EAP

Para solucionar problemas de interação entre a WLC e o servidor de autenticação (servidor RADIUS externo ou EAP interno), use o comando **debug AAA all enable** , que mostra os detalhes necessários. Esse comando é usado após o comando **debug client** e pode ser combinado com outros comandos de depuração conforme necessário (por exemplo, o comando **handoff**).

<#root>

```
(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.
```

Conexão do cliente

Para os fins deste documento, a *conexão do cliente* é o processo para um cliente sem fio passar por estas etapas:

Seção 802.11

1. Sondar, para encontrar um AP válido para associar.
2. Autenticação: pode ser aberta (nula) ou compartilhada. Normalmente, Abrir está selecionado.
3. Associação: solicite serviços de dados ao AP.

Seção Políticas de L2

1. Nenhuma; a autenticação PSK ou EAP ocorre com base na configuração.
2. Negociação de chave, se um método de criptografia for selecionado.

Seção Políticas de L3

1. Aprender endereço.
2. Autenticação da Web, se selecionada.

> **Observação**: essas etapas representam um subconjunto ou resumo do processo completo. Este documento descreve um cenário simplificado que cobre políticas 802.11 e L2 e usa WPA-PSK, além de aprendizagem de endereços. Não são usadas políticas AAA ou L3 externas para autenticação.

Processos do controlador

Em cada seção, o controlador usa processos separados para controlar o estado do cliente em cada momento. Os processos interagem entre eles para garantir que o cliente seja adicionado à tabela de conexão (de acordo com as políticas de segurança configuradas). Para entender as etapas de conexão do cliente com o controlador, aqui está um breve resumo dos processos mais relevantes:

- **Policy Enforcement Module (PEM)** â€” Controla o estado do cliente e o força através de cada uma das políticas de segurança na configuração da WLAN.
- **Access Point Functions (APF)** â€" Basicamente, a máquina de estado 802.11.
- **Dot1x** â€" Implementa a máquina de estado para 802.1x, a autenticação PSK e o identificador de chave para os clientes sem fio.
- **Mobilidade** â€" Rastreia a interação com outros controladores no mesmo grupo de mobilidade.
- **Camada de Transformação de Dados (DTL - Data Transformation Layer)** â€" Fica entre os componentes de software e a aceleração de hardware de rede (NPU - Network Hardware Acceleration); controla as informações ARP.

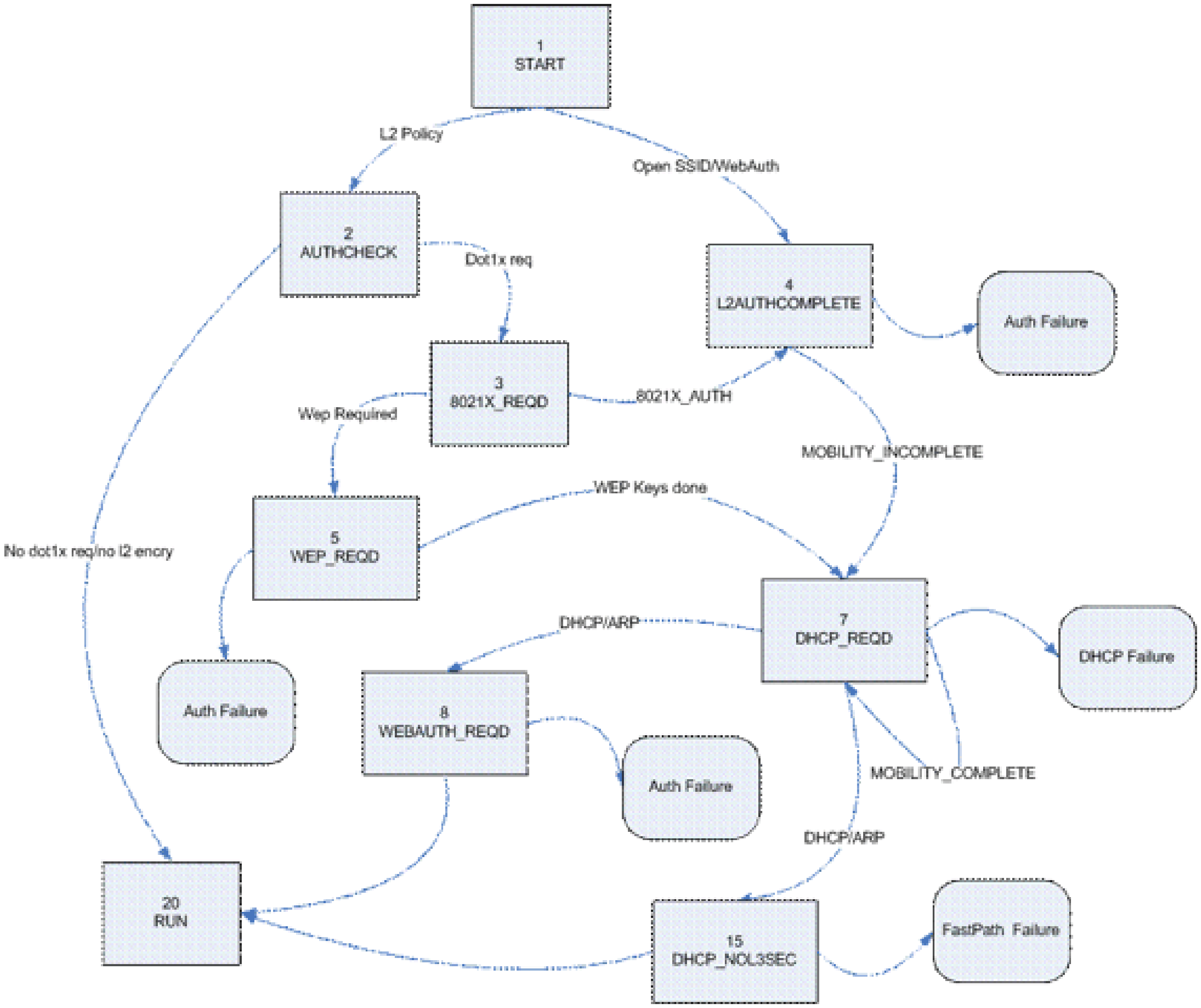
Módulo de aplicação de política (PEM)

Com base na configuração da WLAN, o cliente passa por uma série de etapas. O PEM garante que isso seja feito para estar em conformidade com as políticas de segurança de L2 e L3 necessárias.

Aqui está um subconjunto dos estados PEM relevantes para a análise de uma depuração de cliente:

- **START** â€" Status inicial para entrada de novo cliente.
- **AUTHCHECK** â€" A WLAN tem uma política de autenticação L2 para aplicar.
- **8021X_REQD** â€" O cliente deve concluir a autenticação 802.1x.
- **L2AUTHCOMPLETE** â€" O cliente concluiu com êxito a política L2. O processo agora pode prosseguir para as políticas de L3 (aprendizagem de endereço, autenticação da Web etc.). O controlador envia aqui o anúncio de mobilidade para aprender informações de L3 de outros controladores se este for um roam de cliente no mesmo grupo de mobilidade.
- **WEP_REQD** â€" O cliente deve concluir a autenticação WEP.
- **DHCP_REQD** â€" O controlador precisa aprender o endereço L3 do cliente, o que é feito por solicitação ARP, solicitação ou renovação DHCP ou por informações aprendidas de outro controlador no grupo de mobilidade. Se DHCP necessário estiver marcado na WLAN, somente as informações de DHCP ou mobilidade serão usadas.
- **WEBAUTH_REQD** â€" O cliente deve concluir a autenticação da Web. (política de L3)
- **EXECUTAR** â€" O cliente concluiu com êxito as políticas L2 e L3 necessárias e agora pode transmitir o tráfego para a rede.

Esta imagem mostra uma máquina de estado PEM simplificada com as transições de cliente até alcançar o estado RUN, onde o cliente pode agora enviar tráfego para a rede:



Observação: esta figura não cobre todas as transições e estados possíveis. Para maior clareza, foram suprimidas algumas etapas intermédias.

Encaminhamento de tráfego de cliente

Entre o estado START e antes do estado RUN final, o tráfego do cliente não é encaminhado para a rede, mas é passado para a CPU principal no controlador para análise. As informações encaminhadas dependem do estado e das políticas em vigor; por exemplo, se 802.1x estiver habilitado, o tráfego EAPOL será encaminhado para a CPU. Outro exemplo é se Web Auth for usado, então o HTTP e o DNS são permitidos e interceptados pela CPU para fazer o redirecionamento da Web e obter credenciais de autenticação de cliente.

Quando o cliente alcança o estado RUN, as informações do cliente são enviadas à NPU para permitir a comutação FastPath, que faz um encaminhamento de taxa de cabo do tráfego do usuário para a VLAN do cliente e libera a CPU central das tarefas de encaminhamento de dados do usuário.

O tráfego encaminhado depende do tipo de cliente que é aplicado à NPU. Esta tabela descreve os tipos mais relevantes:

Tipo	Descrição
1	Encaminhamento normal de tráfego de cliente.

9	IP learn state (Estado de aprendizado do IP). Um pacote desse cliente é enviado à CPU para aprender o endereço IP usado.
2	Passagem da ACL. Usada quando a WLAN é uma ACL configurada para informar a NPU.

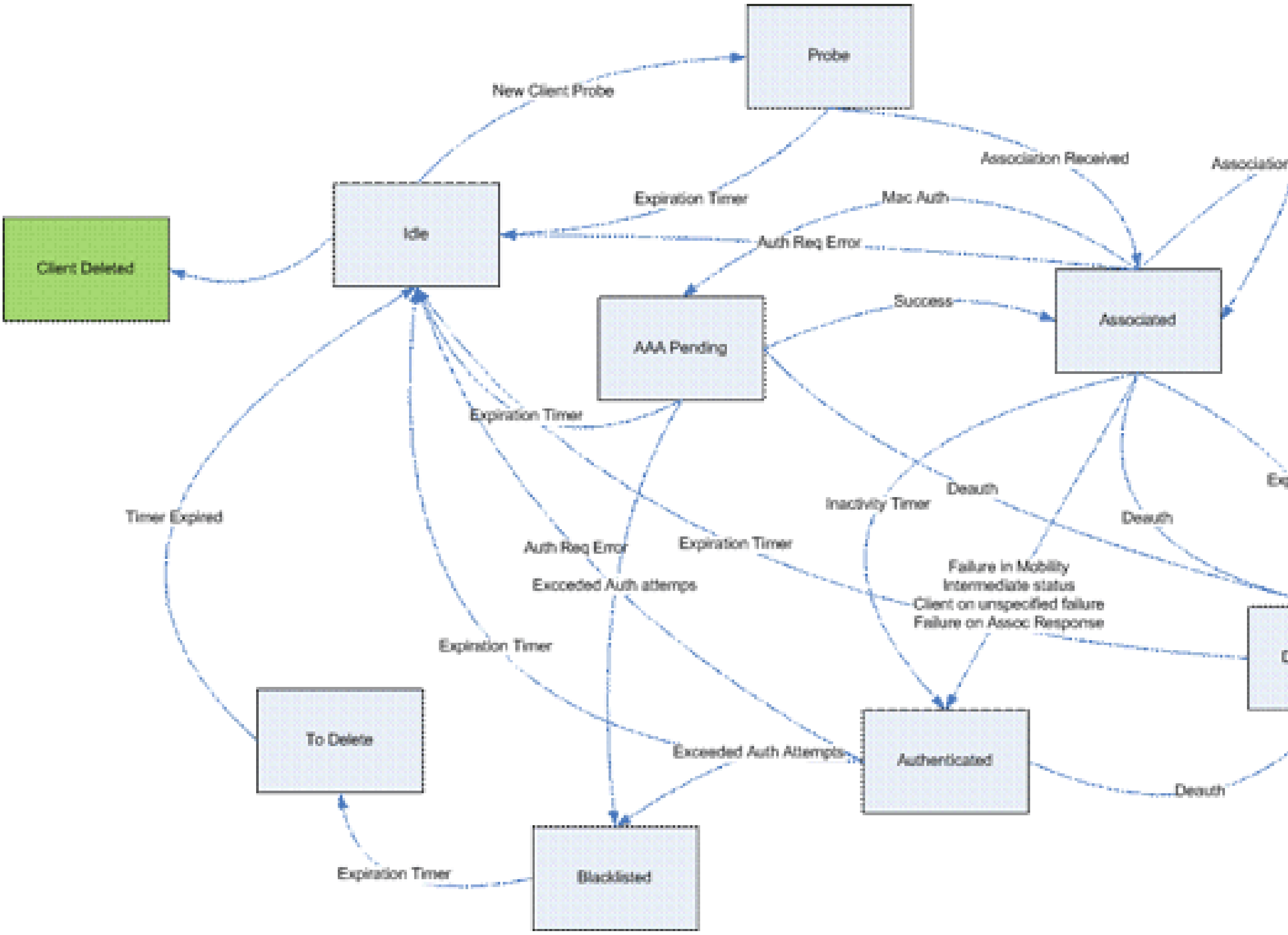
Funções de access point (APF)

Esse processo manipula o estado do cliente por meio do estado da máquina 802.11 e interage com o código de mobilidade para validar os diferentes cenários de roaming. Este documento não aborda os detalhes da mobilidade ou seus estados.

Esta tabela mostra os estados mais relevantes dos clientes que podem ocorrer quando um cliente é associado à controladora:

Nome	Descrição
Ocioso	Novo estado do cliente ou temporário em algumas situações.
Pingente AAA	O cliente aguarda a autenticação do endereço MAC.
Autenticado	Autenticação aberta bem-sucedida ou estado intermediário em algumas situações.
Associado	O cliente passou com êxito os processos de autenticação MAC e de autenticação aberta.
Desassociado	O cliente enviou a desassociação/desautenticação ou o temporizador de associação expirou.
Para excluir	Cliente marcado para ser excluído (normalmente após a expiração do temporizador de exclusão).
Sondar	Solicitação de sondagem recebida para o novo cliente.
Excluído/Bloqueado listado	O cliente foi marcado como excluído. Normalmente relacionado a políticas WPS.
Inválido	Erro no estado do cliente.

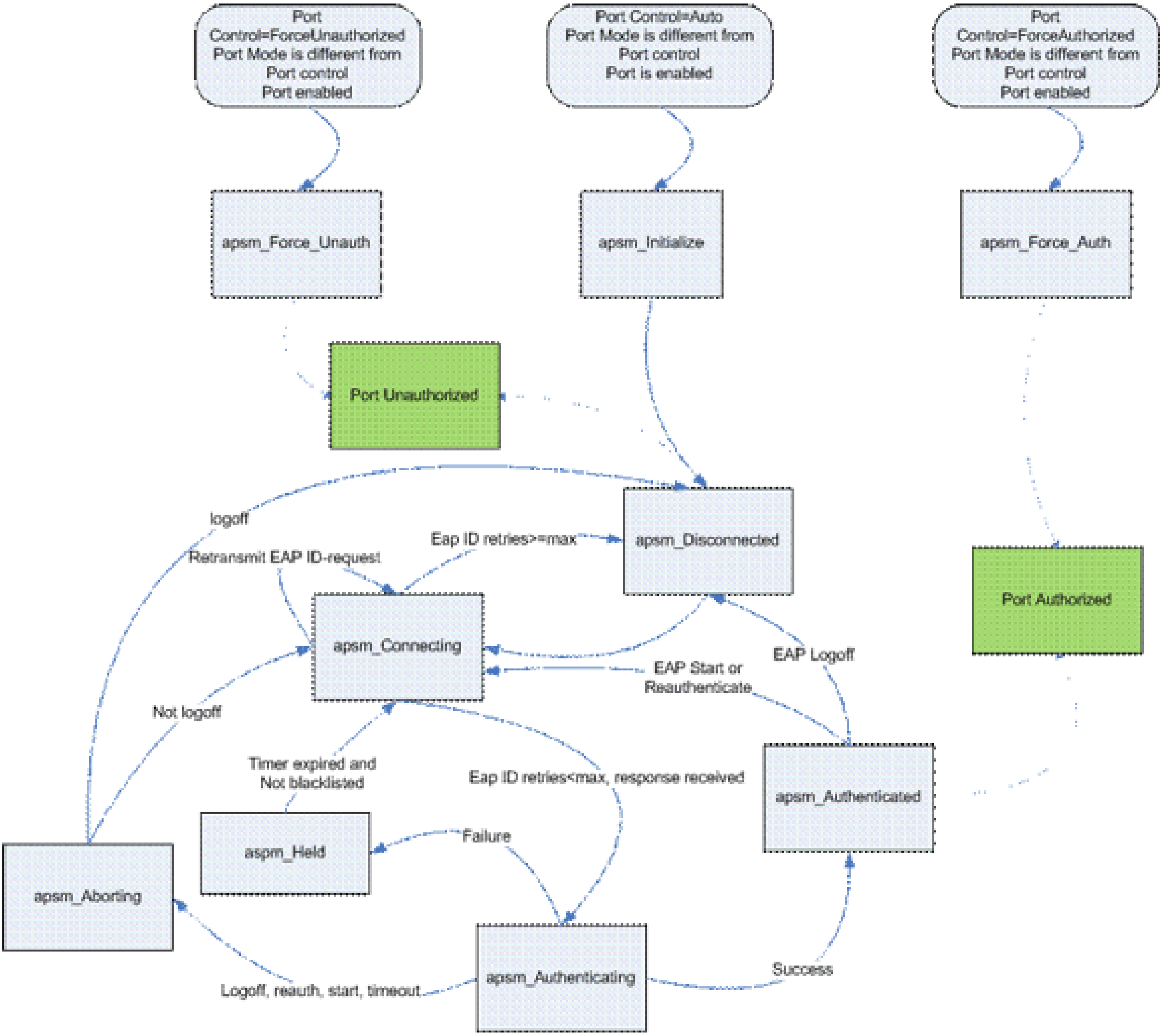
Esta imagem representa uma transição de máquina de estado e mostra apenas os estados e as transições mais relevantes:



Autenticação 802.1x (Dot1x)

O processo Dot1x é responsável pela autenticação 802.1x e pelo gerenciamento de chaves do cliente. Isso significa que, mesmo em WLANs que não tenham uma política EAP que exija 802.1x, o dot1x participa para lidar com a criação e negociação de chave com o cliente e também para o tratamento de chave em cache (PMK ou CCKM).

Esta máquina de estado mostra as transições 802.1x completas:


Port Control=ForceUnauthorized Port Mode is different from Port control Port enabled
Port Control=Auto Port Mode is different from Port control Port is enabled
Port Control=ForceAuthorized Port Mode is different from Port control Port enabled
apsm_Force_Unauth
apsm_Initialize
apsm_Force_Auth
Port Unauthorized
logoff
Retransmit EAP ID-request
Eap ID retries>=max
apsm_Disconnected
Port Authorized
apsm_Connecting
EAP Logoff
EAP Start or Reauthenticate
Not logoff
Timer expired and Not blacklisted
Eap ID retries<max, response received
apsm_Authenticated
aspm_Held
Failure
apsm_Aborting
apsm_Authenticating
Success
Logoff, reauth, start, timeout

Depurar Análise do Cliente

Esta seção mostra o processo completo nos registros quando um cliente se conecta a uma WLAN.

<#root>

```
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 that depend 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
    00.00.00.00.00.00.00.02

!--- 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: x.x.x.x  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: x.x.x.x

!--- 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: x.x.x.x  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.
```

Exemplos de solução de problemas

Configuração incorreta de codificação de cliente

Este exemplo mostra um cliente com diferentes capacidades para o AP. Os testes de cliente para o SSID, mas como a solicitação de teste mostra alguns parâmetros não suportados, o cliente nunca prossegue para as fases de autenticação/associação.

Em particular, o problema apresentado foi uma incompatibilidade entre o cliente que usa WPA e o AP que anuncia apenas o suporte WPA2:

```
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.
```

Chave pré-compartilhada incorreta

Isso mostra que o cliente tenta autenticar pelo WPA-PSK na infraestrutura, mas falha devido à incompatibilidade da chave pré-compartilhada entre o cliente e o controlador, o que resulta na eventual adição do cliente à lista de exclusão (bloqueio):

```
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 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 block listed


Wed Oct 31 10:56:10 2007: 00:1b:77:42:07:69 Block listing (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
```

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.