Compreender debuga o cliente nos controladores do Wireless LAN (os WLC)

Índice

Introdução

Este documento fornece informações detalhadas sobre a saída do comando debug client nos Controllers de LAN Wireless.

Este capas de documento estes assuntos:

- Como um cliente Wireless é tratado
- Pesquisando defeitos edições da associação básica e da autenticação

A saída a ser analisada cobre a encenação para uma rede da chave pré-compartilhada WPA (WPA-PSK).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar o controlador do Wireless LAN (WLC) e o Access point de pouco peso (REGAÇO) para a operação básica
- Métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point
- Como a autenticação do 802.11 e o trabalho de processos de associação

Componentes Utilizados

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

- 2000/2100/4400 Series WLC de Cisco que executa o firmware 4.1 ou 4.2
- Access point LWAPP-baseados

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Debugar o cliente

O cliente do comando debug **<MACADDRESS >** é um macro que permita oito comandos debug, mais um filtro no MAC address fornecido, tão somente as mensagens que contêm o endereço de MAC especificado são mostradas. Os oito comandos debug mostram os detalhes os mais importantes na associação de cliente e na autenticação. O filtro ajuda com situações onde há clientes Wireless múltiplos. As situações como quando demasiada saída é gerada ou o controlador são sobrecarregados quando debugar é permitido sem o filtro.

Os detalhes importantes das tampas da informações recolhidas sobre a associação de cliente e a autenticação (com as duas exceções mencionadas mais tarde neste documento).

Os comandos que são permitidos são mostrados nesta saída:

```
(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.
```

Estes comandos cobrem a negociação de endereços, a máquina de estado do cliente do 802.11, a autenticação do 802.1x, o módulo do reforço de política (PEM), e a negociação de endereços (DHCP).

Debugar variações do cliente

Para a maioria de encenações, os **<MACAddress > o** comando do **cliente debugar** são bastante para obter a informação necessária. Contudo, estão aqui duas situações importantes onde a eliminação de erros adicional é precisada:

- Mobilidade (cliente que vagueia entre controladores)
- Troubleshooting da autenticação de EAP

Mobilidade

Nesta situação, a mobilidade debuga a necessidade de ser permitido depois que os **<MACAddress > o** comando do **cliente debugar** foram introduzidos a fim ganhar a informação adicional na interação do protocolo da mobilidade entre controladores.

Nota: Os detalhes nesta saída serão cobertos nos documentos futuros.

A fim permitir a mobilidade debuga, usam os **<MACAddress do cliente debugar >**, e usam então o **comando enable da entrega da mobilidade debugar**:

```
(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.
```

Troubleshooting da autenticação de EAP

A fim pesquisar defeitos a interação entre o WLC e o Authentication Server (RAIO externo ou server interno EAP), use o comando debug aaa all enable, que mostra os detalhes exigidos. Este comando deve ser usado depois que os **<MACAddress > o** comando do **cliente debugar** e pode ser combinado com os outros comandos de debug como necessário (por exemplo, **entrega**).

```
(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 de cliente

Para fins deste documento, a *conexão de cliente* é o processo para que um cliente Wireless passe com estas etapas:

Seção do 802.11

1. Sondagem, para encontrar um AP válido para associar.
2. Autenticação: Pode estar aberto (zero) ou compartilhou. Normalmente, Open é selecionada.
3. Associação: Pedindo serviços dos dados ao AP.

Seção das políticas L2

1. Nenhum; O PSK ou a autenticação de EAP ocorrem segundo a configuração.
2. Negociação chave, se um método de criptografia é selecionado.

Seção das políticas L3

1. Aprendizagem de endereço.
2. Autenticação da Web, se selecionado.

Nota: Estas etapas representam um subconjunto ou um sumário do processo completo. Este documento descreve uma encenação simplificada que cubra o 802.11 e as políticas L2 e use o WPA-PSK, mais a aprendizagem de endereço. Nenhuma política AAA ou L3 externo para a autenticação é usada.

Processos do controlador

Em cada seção, o controlador usa processos separados a fim manter-se a par do estado do cliente em cada momento. Os processos interagem entre eles para assegurar-se de que o cliente esteja adicionado à tabela de conexão (pelas políticas de segurança configuradas). A fim compreender as etapas da conexão de cliente ao controlador, é aqui um sumário sucinto dos processos os mais relevantes:

- **Módulo do reforço de política (PEM)** — Controla o estado do cliente e força-o com cada um das políticas de segurança na configuração WLAN.
- **Funções do Access point (APF)** — Basicamente, a máquina de estado do 802.11.
- **Dot1x** — Executa a máquina de estado para o 802.1x, a autenticação PSK, e a chave que segura para os clientes Wireless.
- **Mobilidade** — Segue a interação com outros controladores no mesmo grupo da mobilidade.
- **Camada da transformação dos dados (DTL)** — Senta-se entre os componentes de software e a aceleração do hardware de rede (NPU); controla a informação ARP.

Módulo do reforço de política (PEM)

Baseado na configuração WLAN, o cliente passa com uma série de etapas. O PEM assegura-se de que este esteja feito para que siga com as políticas de segurança L2 e L3 exigidas.

Está aqui um subconjunto dos estados PEM relevantes para a análise de um cliente debuga:

- **COMEÇO** — Estado inicial para a entrada de cliente nova.
- **AUTHCHECK** — O WLAN tem uma política de autenticação L2 a reforçar.
- **8021X_REQD** — O cliente deve terminar a autenticação do 802.1x.
- **L2AUTHCOMPLETE** — O cliente terminou com sucesso a política L2. O processo pode agora continuar às políticas L3 (aprendizagem de endereço, AUTH da Web, etc.). O controlador envia aqui o anúncio da mobilidade para aprender a informação L3 de outros controladores se este é um cliente vagueando no mesmo grupo da mobilidade.
- **WEP_REQD** — O cliente deve terminar a autenticação WEP.
- **DHCP_REQD** — O controlador precisa de aprender o endereço L3 do cliente, que é feito pela requisição ARP, requisição DHCP ou renova, ou pela informação aprendida do outro controlador no grupo da mobilidade. Se o DHCP exigido é marcado no WLAN, simplesmente a informação DHCP ou de mobilidade está usada.
- **WEBAUTH_REQD** — O cliente deve terminar a autenticação da Web. (Política L3)
- **SEJA EXECUTADO** — O cliente terminou com sucesso as políticas L2 e L3 exigidas e pode agora transmitir o tráfego à rede.

Esta figura mostra uma máquina de estado simplificada PEM com as transições do cliente até que alcance o estado de CORRIDA, onde o cliente pode agora enviar o tráfego à rede:

Nota: Esta figura não cobre todas as transições e estados possíveis. Algumas etapas intermediárias foram removidas para maior clareza.

Encaminhamento de tráfego do cliente

Entre o estado do COMEÇO e antes do estado de CORRIDA final, o tráfego do cliente não é enviado à rede, mas é passado ao CPU principal no controlador para a análise. A informação que é enviada depende do estado e das políticas no lugar; por exemplo, se o 802.1x é permitido, o tráfego EAPOL é enviado ao CPU. Um outro exemplo é se o AUTH da Web é usado, a seguir o HTTP e o DNS estão permitidos e interceptados pelo CPU para fazer a reorientação da Web e obter credenciais da authenticação do cliente.

Quando o cliente alcança o estado de CORRIDA, a informação cliente está enviada ao NPU a fim permitir o interruptor do caminho rápido, que faz uma transmissão da cabo-taxa do tráfego de usuário ao cliente VLAN e livra o CPU central de tarefas da transmissão dos dados do usuário.

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

Tipo	Descrição
1	Encaminhamento de tráfego normal do cliente.
9	Estado de aprendizagem IP. Um pacote deste cliente é enviado ao CPU a fim aprender o endereço IP de Um ou Mais Servidores Cisco ICM NT usado.
2	ACL passagem-através de. Usado quando o WLAN for um ACL configurado para informar o NPU.

O Access point funciona (o APF)

Este processo segura o estado do cliente através do estado da máquina do 802.11 e interage com o código da mobilidade a fim validar as encenações vagueando diferentes. Este documento não cobre os detalhes da mobilidade ou seus estados.

A tabela a seguir mostra os estados do cliente mais relevantes que são entrados dentro durante uma associação de cliente ao controlador:

Nome	Descrição
Ocioso	Cliente ou estado temporário novo em algumas situações.
AAA pendente	Autenticação de espera do MAC address do cliente.
Autenticado	Autenticação aberta bem sucedida ou estado intermediário em algumas situações.
Associado	AUTH com sucesso passado do cliente MAC e processos abertos do AUTH.

Dissociado	Cliente a desassociação/deauthentication enviados temporizador, ou da associação expirou.
Para suprimir	Cliente marcado para ser suprimido (normalmente após o temporizador da exclusão expirou).
Ponta de prova	Pedido da ponta de prova recebido para o cliente novo.
Excluído/põr	O cliente foi marcado como excluído. Relativo normalmente às políticas WPS.
Inválido	Erro no estado do cliente.

Esta figura representa uma transição da máquina de estado e mostra somente a maioria estados relevantes e de transições:

autenticação do 802.1x (dot1x)

O processo do dot1x é responsável para a autenticação e o gerenciamento chave do 802.1x para o cliente. Isto significa que, mesmo nos WLAN que não têm uma política EAP que exige o 802.1x, o dot1x participa para segurar a criação e a negociação chaves com cliente e igualmente para a manipulação posta em esconderijo da chave (PMK ou CCKM).

Esta máquina de estado mostra as transições completas do 802.1x:

Debugar a análise do cliente

```
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 00.00.00.00.00.00.00.02 *!--- 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.*

Exemplos de troubleshooting

Configuração errada da cifra do cliente

Este exemplo mostra um cliente com capacidades diferentes ao AP. O cliente está sondando para o SSID, mas como o pedido da ponta de prova mostra alguns parâmetros não apoiados, o cliente nunca continua às fases da autenticação/associação. Em particular, o problema introduzido era uma má combinação entre o cliente que usa o WPA, e o AP que anuncia somente o apoio 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 Preshared errada

Isto mostra o cliente que tentam autenticar pelo WPA-PSK à infraestrutura, mas a falha devendo combinar mal da chave preshared entre o cliente e o controlador, resultando em põr eventual do cliente:

```
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 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
```

Informações Relacionadas

- Access point de pouco peso FAQ
- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Cisco Wireless LAN Controller Module - Perguntas e Respostas
- Controlador do Wireless LAN (WLC) FAQ
- Gerência de recursos de rádio sob redes Wireless unificadas
- Suporte por tecnologia do Wireless LAN (WLAN)
- Suporte Técnico e Documentação - Cisco Systems