Solucionar problemas de um AP leve que não ingressa em um WLC

Contents

Introdução

Este documento descreve o processo de descoberta e junção do AireOS Wireless LAN Controller (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de Pontos de Acesso Lightweight (LAPs) e WLCs Cisco AireOS
- Conhecimento básico do Lightweight Access Point Protocol (CAPWAP)

Componentes Utilizados

Este documento se concentra nas WLCs AireOS e não cobre o Catalyst 9800, embora o processo de junção seja basicamente semelhante.

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.

Visão geral do processo de descoberta e união de WLC

Em uma rede sem fio unificada da Cisco, os LAPs devem primeiro detectar e se juntarem ao WLC para poderem atender os clientes sem fio.

No entanto, isso apresenta uma pergunta: como os LAPs encontraram o endereço IP de gerenciamento do controlador quando ele estava em uma sub-rede diferente?

Se você não informar ao LAP onde o controlador está por meio da opção de DHCP 43, da resolução do Sistema de Nome de Domínio (DNS - Domain Name System) Cisco-capwap-controller.local_domain ou configurá-lo estaticamente, o LAP não saberá onde encontrar na rede a interface de gerenciamento do controlador.

Além desses métodos, o LAP procura automaticamente na sub-rede local os controladores com um broadcast local de 255.255.255.255. Além disso, o LAP se lembra do endereço IP de gerenciamento de seu controlador e dos controladores presentes como pares de mobilidade, mesmo em reinicializações. No entanto, assim que o AP se une a outra WLC, ele apenas se lembra do IP dessa nova WLC e de seus pares de mobilidade, e não dos anteriores. Portanto, se você colocar o LAP primeiro na sub-rede local da interface de gerenciamento, ele encontrará a interface de gerenciamento do controlador e memorizará o endereço. Isso é chamado de fornecimento. Isso não ajudará a encontrar o controlador se você substituir um LAP posteriormente. Portanto, a Cisco recomenda o uso da opção 43 do DHCP ou dos métodos DNS.

Os LAPs sempre se conectam ao endereço da interface de gerenciamento do controlador primeiro com uma solicitação de detecção. Em seguida, o controlador informa ao LAP o endereço IP da interface do gerenciador de AP da camada 3 (que também pode ser o gerenciamento por padrão) para que o LAP possa enviar uma solicitação de junção à interface do gerenciador de AP.

O AP passa por este processo na inicialização:

- **O LAP inicializa e usa DHCPs em um endereço IP se ele não tiver sido atribuído anteriormente como um endereço IP**

estático.

- **O LAP envia uma solicitação de detecção para os controladores através de vários algoritmos de detecção e cria uma lista de controladores. Essencialmente, o LAP informa o máximo de endereços de interface de gerenciamento que for possível para a lista de controladores através do seguinte:**

a. **Opção de DHCP 43 (boa para empresas globais onde escritórios e controladores estão em continentes diferentes).**

b. **Entrada DNS para** cisco-capwap-controller (boa para empresas locais - também pode ser usada para descobrir onde APs novíssimos se unem) Se você usa CAPWAP, certifique-se de que haja uma entrada DNS para cisco-capwap-controller.

- **Endereços IP de gerenciamento dos controladores que o LAP recorda previamente.**
- **Um broadcast da camada 3 na sub-rede.**
- **Informações configuradas estaticamente.**
- **Os controladores presentes no grupo de mobilidade da WLC em que o AP entrou pela última vez.**

Nessa lista, o método mais fácil de usar para implantação é ter os LAPs na mesma sub-rede que a interface de gerenciamento do controlador e permitir que o broadcast da camada 3 dos LAPs encontre o controlador. Esse método deve ser usado para empresas que têm uma rede pequena e não possuem um servidor DNS local.

O próximo método de implantação mais fácil é usar uma entrada de DNS com DHCP. Você pode ter entradas múltiplas do mesmo nome de DNS. Isso permite que o LAP detecte vários controladores. Esse método deve ser usado por empresas que tenham todos os seus controladores em um único local e possuam um servidor DNS local. Ou, se a empresa tiver vários sufixos DNS e os controladores estiverem segregados por sufixo.

A opção de DHCP 43 é usada por grandes empresas para localizar as informações pelo DHCP. Esse método é usado por grandes empresas que possuem um sufixo DNS único. Por exemplo, a Cisco possui edifícios na Europa, na Austrália e nos Estados Unidos. Para garantir que os LAPS se juntem apenas a controladores localmente, a Cisco não pode usar uma entrada de DNS e deve usar as informações da opção 43 de DCHP para informar os LAPs qual é o endereço IP de gerenciamento de seu controlador local.

Finalmente, a configuração estática é usada para uma rede que não tenha um servidor DHCP. Você pode configurar estaticamente as informações necessárias para se unir a uma controladora pela porta de console e pela CLI dos APs. Para obter informações sobre como configurar estaticamente as informações da controladora usando a CLI do AP, use este comando:

```
AP#capwap ap primary-base <WLCName> <WLCIP>
```

Para obter informações sobre como configurar a opção de DHCP 43 em um servidor DHCP, consulte o exemplo de configuração da opção de DHCP 43

- Envie uma solicitação de detecção a cada controlador na lista e aguarde a resposta de detecção do controlador que contém o nome do sistema, os endereços IP do gerenciador de AP, o número de APs já conectados a cada interface do gerenciador de AP e a capacidade total em excesso do controlador.

- Veja a lista de controladores e envie uma solicitação de junção a um controlador nessa ordem (apenas se o AP recebeu uma resposta de detecção dele):

a. Nome do sistema do controlador primário (configurado anteriormente no LAP).

b. Nome do sistema do controlador secundário (configurado anteriormente no LAP).

c. Nome do sistema do controlador terciário (configurado anteriormente no LAP).

d. Controlador primário (se o LAP não tiver sido configurado anteriormente com nenhum nome de controlador primário, secundário ou terciário). Usado para sempre saber qual controlador é uma junção totalmente nova de LAPs).

e. Se nenhuma das condições anteriores for observada, faça o balanceamento de carga entre os controladores usando o valor de capacidade excedente na resposta de detecção.

Se dois controladores tiverem a mesma capacidade excedente, envie a solicitação de junção para o primeiro controlador que respondeu à solicitação de detecção com uma resposta de detecção. Se um único controlador tiver vários gerenciadores AP em várias interfaces, escolha a interface do gerenciador AP com o menor número de APs.

O controlador responde a todas as solicitações de descoberta sem uma verificação de certificado ou credenciais de AP. No entanto, as solicitações de junção devem ter um certificado válido para obter uma resposta de junção do controlador. Se o LAP não receber uma resposta de junção de sua escolha, ele tentará o próximo controlador na lista, a menos que o controlador seja um controlador configurado (primário/secundário/terciário).

- Quando recebe a resposta da junção, o AP verifica se possui a mesma imagem que a do controlador. Se não tiver, o AP faz o download da imagem a partir do controlador e reinicializa para carregar a nova imagem e inicia o processo novamente a partir da etapa 1.

- Se tiver a mesma imagem do software, ele pedirá a configuração ao controlador e mudará para o estado registrado no controlador.

Depois de baixar a configuração, o AP pode recarregar novamente para aplicar a nova configuração. Portanto, um recarregamento extra poderá ocorrer. Isso é um comportamento normal.

Depurar do controlador

Há alguns **debug** comandos no controlador que você pode usar para ver todo este processo na CLI:

-

debug capwap events enable: mostra pacotes de descoberta e pacotes de junção.

- **debug capwap packet enable**: mostra informações de nível de pacote dos pacotes de descoberta e junção.

- **debug pm pki enable**: mostra o processo de validação do certificado.

- **debug disable-all**: desativa depurações.

Com um aplicativo de terminal que possa capturar a saída para um arquivo de registro, acesse o console ou secure shell (SSH)/Telnet para o controlador e insira estes comandos:

<#root>

config session timeout 120

config serial timeout 120

show run-config

(and spacebar thru to collect all)

debug mac addr <ap-radio-mac-address>

(in xx:xx:xx:xx:xx format)

debug client <ap-mac-address>

debug capwap events enable

debug capwap errors enable

debug pm pki enable

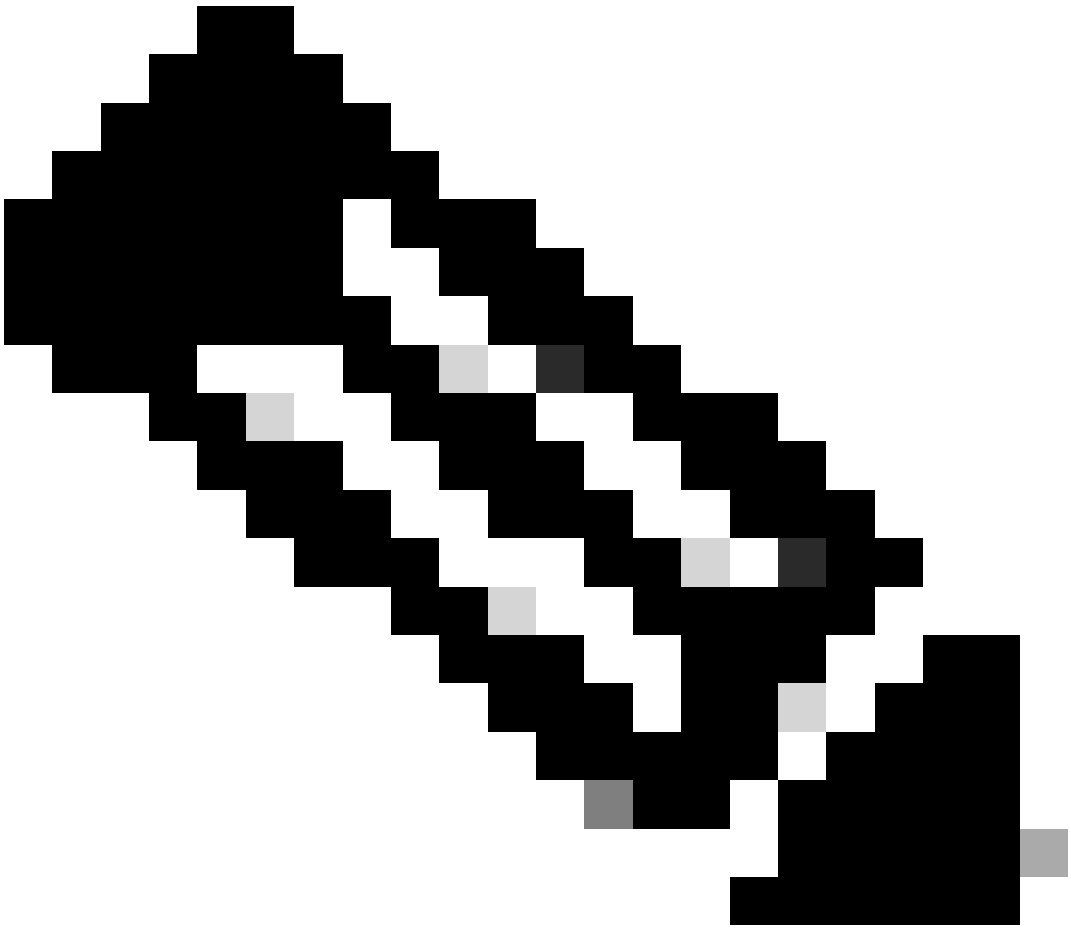
Depois que as depurações forem capturadas, use o comandodebug disable-all para desativar todas as depurações.

As próximas seções mostram a saída desses **debug** comandos quando o LAP se registra com o controlador.

debug capwap events enable

Este comando fornece informações sobre os eventos e erros CAPWAP que ocorrem no processo de junção e descoberta CAPWAP.

Esta é a saída do **debug capwap events enable** comando para um LAP que tem a mesma imagem que o WLC:



Observação: algumas linhas da saída foram movidas para a segunda linha devido a restrições de espaço.

<#root>

debug capwap events enable

*spamApTask7: Jun 16 12:37:36.038: 00:62:ec:60:ea:20 Discovery Request from 172.16.17.99:46317

!--- CAPWAP discovery request sent to the WLC by the LAP.

*spamApTask7: Jun 16 12:37:36.039: 00:62:ec:60:ea:20 Discovery Response sent to 172.16.17.99 port 46317

!--- WLC responds to the discovery request from the LAP.

*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

!--- LAP sends a join request to the WLC.

*spamApTask7: Jun 16 12:38:33.039: 00:62:ec:60:ea:20 Join Priority Processing status = 0, Incoming Ap's
*spamApTask7: Jun 16 12:38:43.469: 00:62:ec:60:ea:20 Join Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.472: 00:62:ec:60:ea:20 Join Version: = 134256640

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 apType = 46 apModel: AIR-CAP2702I-E-K9

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join resp: CAPWAP Maximum Msg element len = 90

*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 Join Response sent to 172.16.17.99:46317
*spamApTask7: Jun 16 12:38:43.473: 00:62:ec:60:ea:20 CAPWAP State: Join

!--- WLC responds with a join reply to the LAP.

```
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Configuration Status from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 CAPWAP State: Configure
```

!--- LAP requests for the configuration information from the WLC.

```
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP info for AP 00:62:ec:60:ea:20 -- stati
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Updating IP 172.16.17.99 ===> 172.16.17.99 for AP
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Running spamDecodeVlanProfMapPayload for00:62:ec:6
*spamApTask7: Jun 16 12:38:43.964: 00:62:ec:60:ea:20 Setting MTU to 1485
*spamApTask7: Jun 16 12:38:44.019: 00:62:ec:60:ea:20 Configuration Status Response sent to 172:16:17:99
```

!--- WLC responds by providing all the necessary configuration information to the LAP.

```
*spamApTask7: Jun 16 12:38:46.882: 00:62:ec:60:ea:20 Change State Event Request from 172.16.17.99:46317

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Radio state change for slot: 0 state: 2 cause: 0 d
*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Change State Event Response sent to 172.16.17.99:4
.
.
.
.

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 CAPWAP State: Run

*spamApTask7: Jun 16 12:38:46.883: 00:62:ec:60:ea:20 Sending the remaining config to AP 172.16.17.99:46
.
.
.
.
```

!--- LAP is up and ready to service wireless clients.

```
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmInterferen
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmNeighbourC
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for RrmReceiveCtr
*spamReceiveTask: Jun 16 12:38:46.897: 00:62:ec:60:ea:20 Configuration update request for CcxRmMeas pay
```

!--- WLC sends all the RRM and other configuration parameters to the LAP.

Como mencionado na seção anterior, quando um LAP tiver se registrado com um WLC, ele verificará para saber se tem a mesma imagem que o controlador. Se as imagens no LAP e no WLC forem diferentes, os LAPs farão o download da nova imagem a partir do WLC primeiro. Se o LAP tiver a mesma imagem, ele continuará a fazer o download da configuração e de outros parâmetros a partir do WLC.

Você verá essas mensagens na saída do **debug capwap events enable** comando se o LAP baixar uma imagem da controladora como parte do processo de registro:

```
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Sending image data block of length 1324 and msgLen
*spamApTask6: Jun 17 14:23:28.677: 00:62:ec:60:ea:20 Image Data Request sent to 172.16.17.201:46318
*spamApTask6: Jun 17 14:23:28.693: 00:62:ec:60:ea:20 Image data Response from 172.16.17.201:46318
```

Quando o download da imagem estiver concluído, o LAP será reinicializado, executará a descoberta e ingressará no algoritmo novamente.

debug pm pki enable

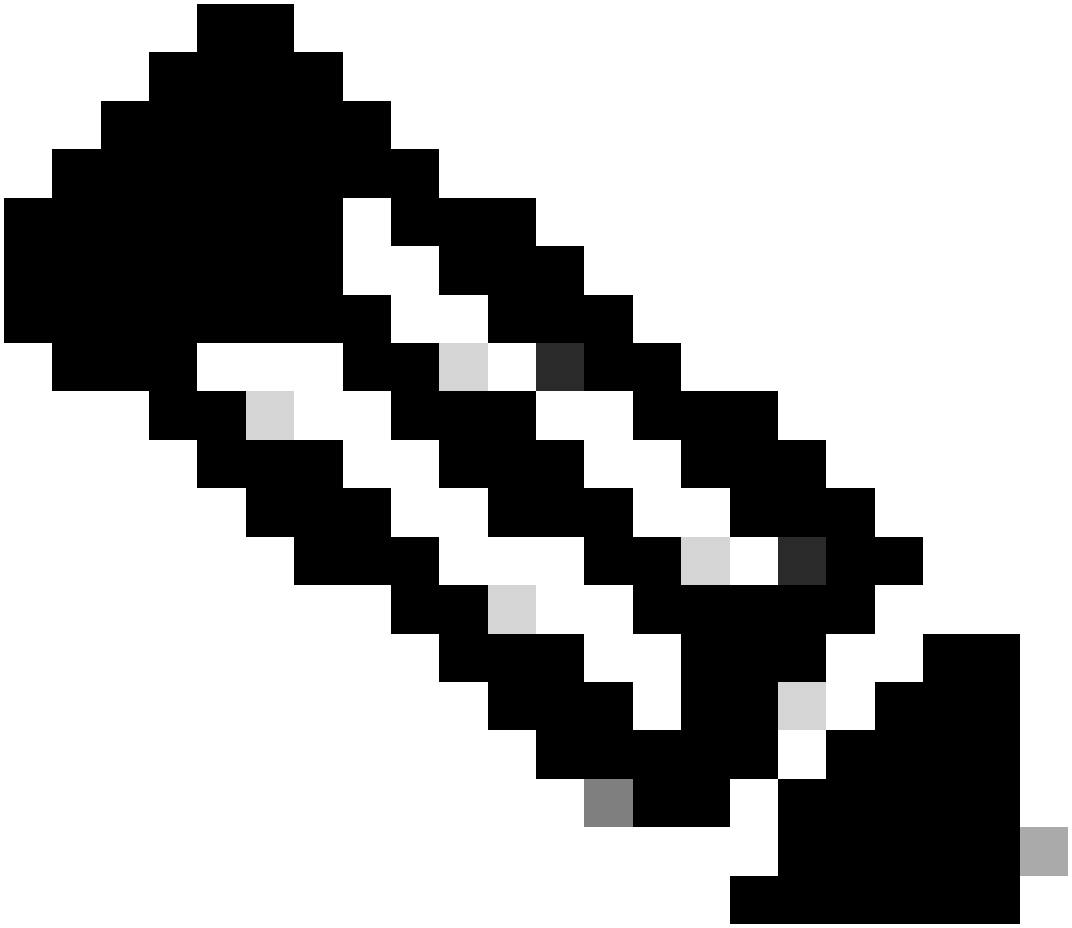
Como parte do processo de junção, a WLC autentica cada LAP confirmando que seu certificado é válido.

Quando o AP envia a solicitação de junção CAPWAP para a WLC, ele incorpora seu certificado X.509 na mensagem CAPWAP. O AP também gera um ID de sessão aleatório que também é incluído na solicitação de junção do CAPWAP. Quando a WLC recebe a solicitação de junção do CAPWAP, ela valida a assinatura do certificado X.509 com a chave pública do AP e verifica se o certificado foi emitido por uma autoridade de certificação confiável.

Ele também examina a data e a hora de início do intervalo de validade do certificado AP e compara essa data e hora com sua própria data e hora

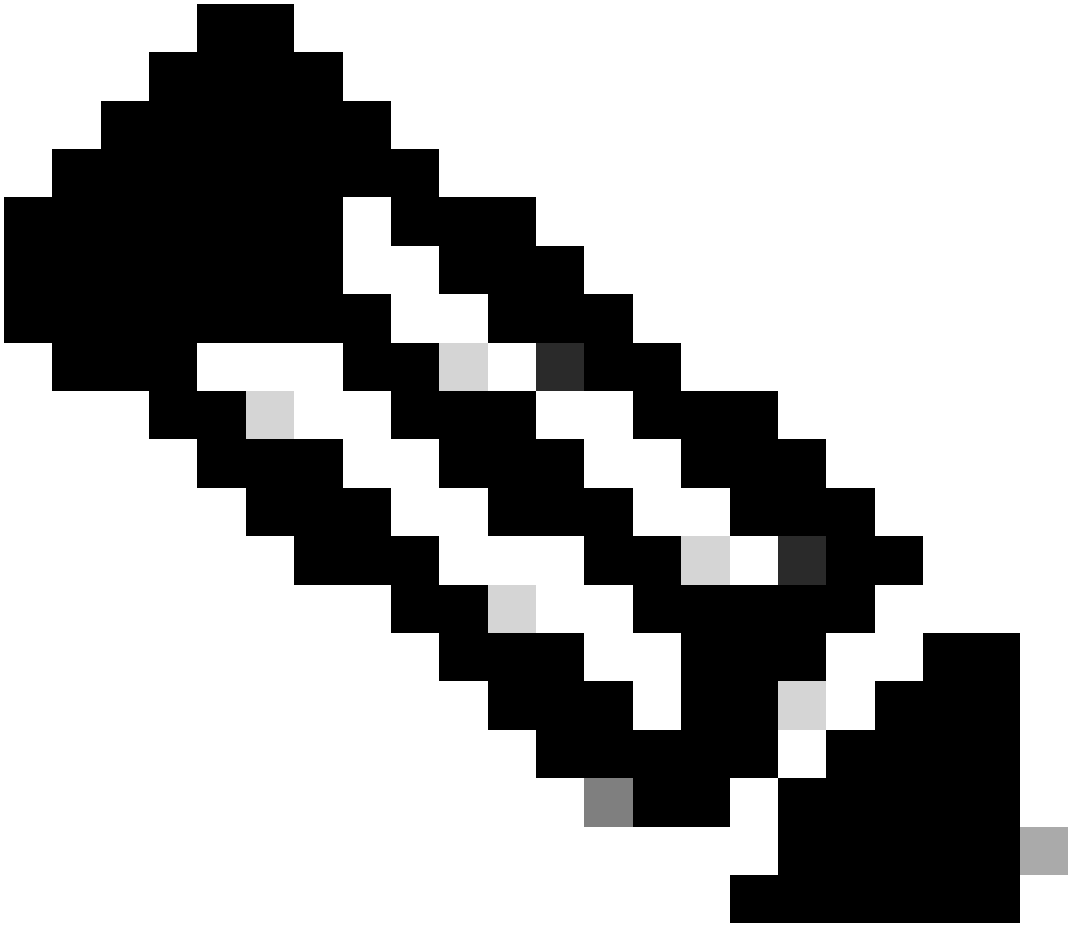
(portanto, o relógio do controlador precisa ser definido próximo à data e hora atuais). Se o certificado X.509 for validado, o WLC gerará uma chave de criptografia AES aleatória. A WLC insere as chaves AES em seu mecanismo de criptografia para que possa criptografar e descriptografar futuras mensagens de controle do CAPWAP trocadas com o AP. Observe que os pacotes de dados são enviados no túnel CAPWAP entre o LAP e o controlador.

O **debug pm pki enable** comando mostra o processo de validação de certificação que ocorre na fase de junção no controlador. O **debug pm pki enable** comando também exibe a chave hash do AP no processo de junção, se o AP tiver um certificado autoassinado (SSC) criado pelo programa de conversão LWAPP. Se o AP tiver um Certificado de instalação fabricada (MIC), você não verá uma chave de hash.



Observação: todos os APs fabricados após junho de 2006 têm um MIC.

Esta é a saída do **debug pm pki enable** comando quando o LAP com um MIC se une à controladora:



Observação: algumas linhas da saída foram movidas para a segunda linha devido a restrições de espaço.

<#root>

```
*spamApTask4: Mar 20 11:05:15.687: [SA] OpenSSL Get Issuer Handles: locking ca cert table

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: x509 subject_name /C=US/ST=Californ
CN=AP3G2-1005cae83a42/emailAddress=support@cisco.com
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

issuer_name /O=Cisco Systems/CN=Cisco Manufacturing CA

```
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: CN AP3G2-1005cae83a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: issuerCertCN Cisco Manufacturing CA
*spamApTask4: Mar 20 11:05:15.688: [SA] GetMac: MAC: 1005.cae8.3a42
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: openssl Mac Address in subject is 1
*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Cert Name in subject is AP3G2-1005c

*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles: Extracted cert issuer from subject


*spamApTask4: Mar 20 11:05:15.688: [SA] OpenSSL Get Issuer Handles:
```

Cert is issued by Cisco Systems.

```
*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultMfgCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row
*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 260e5e69 for certname cscoDefaultMfgCaCert

*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultMfgCaCert in row 5 x

*spamApTask4: Mar 20 11:05:15.688: [SA] Retrieving x509 cert for CertName cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: called to evaluate <cscoDefaultNewRootCaCert>
*spamApTask4: Mar 20 11:05:15.688: [SA] sshpmGetCID: Found matching CA cert cscoDefaultNewRootCaCert in

*spamApTask4: Mar 20 11:05:15.688: [SA] Found CID 28d7044e for certname cscoDefaultNewRootCaCert
*spamApTask4: Mar 20 11:05:15.688: [SA] CACertTable: Found matching CID cscoDefaultNewRootCaCert in row
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification return code: 1
*spamApTask4: Mar 20 11:05:15.691: [SA] Verify User Certificate: X509 Cert Verification result text: ok
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultMfgCaCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching CA cert cscoDefaultMfgCaCert in row

*spamApTask4: Mar 20 11:05:15.691: [SA]
```

Verify User Certificate: OPENSSL X509_Verify: AP Cert Verfied Using >cscoDefaultMfgCaCert<

```
*spamApTask4: Mar 20 11:05:15.691: [SA] OpenSSL Get Issuer Handles:
```

Check cert validity times (allow expired NO)

```
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: called to evaluate <cscoDefaultIdCert>
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmGetCID: Found matching ID cert cscoDefaultIdCert in row 2
*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle: called with 0x1b0b9380

*spamApTask4: Mar 20 11:05:15.691: [SA] sshpmFreePublicKeyHandle:
```

freeing public key

Depurar a partir do AP

Se as depurações do controlador não indicarem uma solicitação de junção, você poderá depurar o processo do AP se o AP tiver uma porta de console. Você pode ver o processo de inicialização do AP com esses comandos, mas primeiro você deve entrar no modo de ativação (a senha padrão é Cisco).

- **debug dhcp detail** : mostra informações da opção 43 do DHCP.
- **debug ip udp**: mostra todos os pacotes UDP recebidos e transmitidos pelo AP.
- debug capwap client event : mostra eventos capwap para o AP.
- **debug capwap client error**: mostra erros de capwap para AP.

- **debug dtls client event**: mostra eventos DTLS para o AP.
- **debug dtls error enable**: mostra erros DTLS para o AP.
- **undebug all**: desabilita depurações no AP.

Aqui está um exemplo da saída dos debug capwapcomandos. Essa saída parcial dá uma ideia dos pacotes enviados pelo AP no processo de inicialização para descobrir e se unir a um controlador.

<#root>

```
AP can discover the WLC via one of these options :
```

!--- AP discovers the WLC via option 43

```
*Jun 28 08:43:05.839: %CAPWAP-5-DHCP_OPTION_43: Controller address 10.63.84.78 obtained through DHCP
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.78 with discovery type set
```

!--- capwap Discovery Request using the statically configured controller information.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 10.63.84.32 with discovery type set
```

!--- Capwap Discovery Request sent using subnet broadcast.

```
*Jun 28 08:43:15.963: %CAPWAP-3-EVENTLOG: Discovery Request sent to 255.255.255.255 with discovery type
```

!--- capwap Join Request sent to AP-Manager interface on DHCP discovered controller.

```
*Jun 28 08:40:29.031: %CAPWAP-5-SENDJOIN: sending Join Request to 10.63.84.78
```

O LAP não se junta ao controlador, por quê?

Verifique os princípios básicos primeiro

- O AP e o WLC podem se comunicar?
- Certifique-se de que o AP receba um endereço do DHCP (verifique as concessões do servidor DHCP para o endereço MAC do AP).
- Faça ping no AP a partir da controladora.
- Verifique se a configuração do STP no switch está correta, de modo que os pacotes para as VLANs não sejam bloqueados.
- Se os pings forem bem sucedidos, assegure-se de que o AP tenha pelo menos um método pelo qual detectar pelo menos um console WLC único ou use telnet/ssh no controlador para executar a depuração.
-

Cada vez que o AP é reinicializado, ele inicia a sequência de descoberta da WLC e tenta localizar o AP. Reinicialize o AP e verifique se ele se une à WLC.

Aqui estão alguns dos problemas mais comuns encontrados devido aos quais os LAPs não se juntarão ao WLC.

Field Notice: Expirações do Certificado - FN63942

Os certificados incorporados ao hardware são válidos por um período de 10 anos após a fabricação. Se seus APs ou WLC tiverem mais de 10 anos, os certificados expirados podem causar problemas de ingresso no AP. Mais informações sobre esse problema estão disponíveis neste field notice: Field Notice: FN63942.

Possíveis problemas a serem procurados: Exemplos

Problema 1: A hora do controlador está fora do intervalo de validade do certificado

Conclua estas etapas para solucionar esse problema:

- Emita debug dtls client error + debug dtls client event comandos no AP:

<#root>

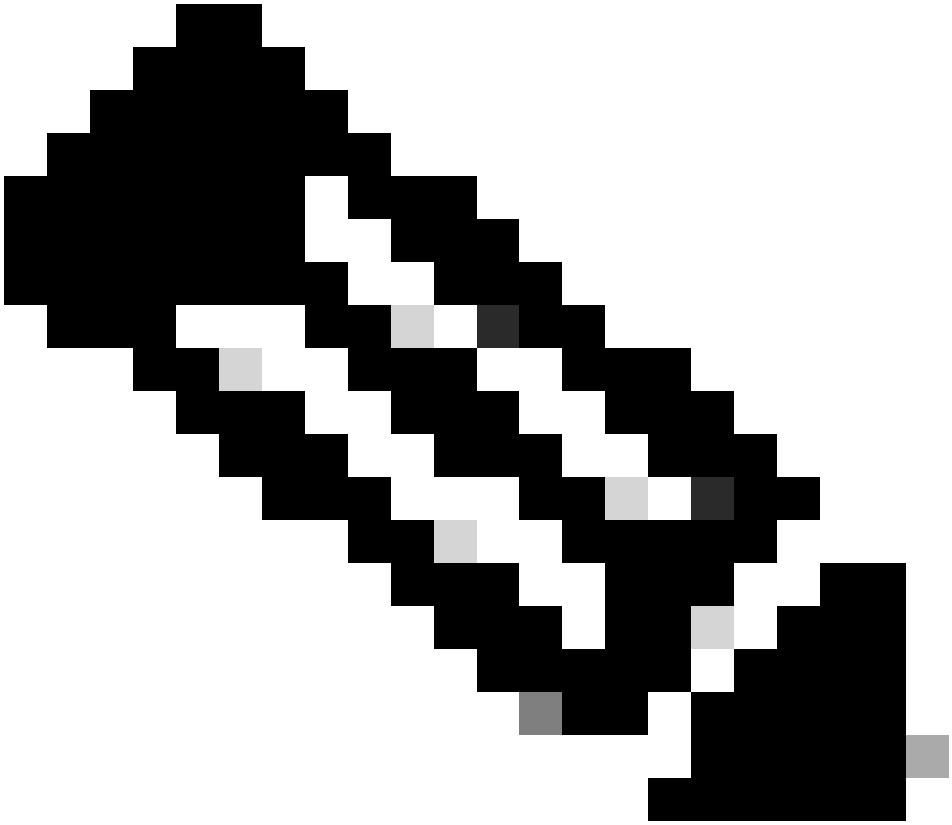
```
*Jun 28 09:21:25.011: DTLS_CLIENT_EVENT: dtls_process_Certificate: Processing...Peer certificate v
*Jun 28 09:21:25.031: DTLS_CLIENT_ERROR: ../capwap/base_capwap/capwap/base_capwap_wtp_dtls.c:509 C
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL :
```

Bad certificate Alert

```
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_client_process_record: Error processing Certificate.
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x8AE7FD0
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_free_connection: Free Called... for Connection 0x8AE
*Jun 28 09:21:25.031: DTLS_CLIENT_EVENT: dtls_send_Alert: Sending FATAL : Close notify Alert
```

Essas informações mostram claramente que a hora do controlador está fora do intervalo de validade do certificado do AP. Portanto, o AP não pode se registrar com a controladora. Os certificados instalados no AP têm um intervalo de validade predefinido. A hora do controlador deve ser definida para que esteja dentro do intervalo de validade do certificado do AP.

- Execute o **show time** comando da CLI da controladora para verificar se a data e a hora definidas em sua controladora estão dentro desse intervalo de validade. Se a hora do controlador for maior ou menor do que esse intervalo de validade do certificado, altere a hora do controlador para que fique dentro desse intervalo.



Observação: se a hora não estiver definida corretamente na controladora, escolha Commands > Set Time no modo GUI da controladora ou execute o comando config time na CLI da controladora para definir a hora da controladora.

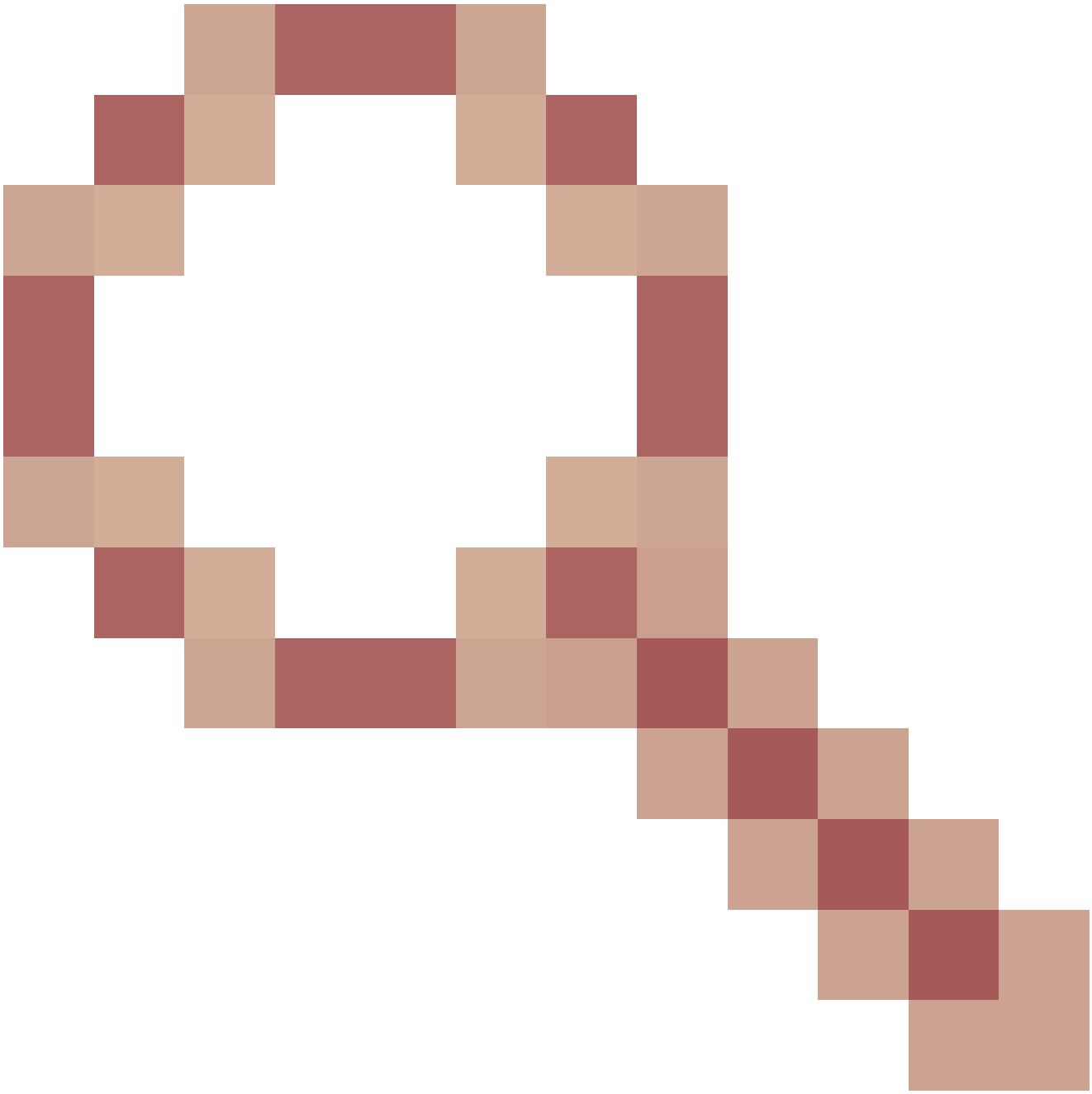
- Em APs com acesso à CLI, verifique os certificados com o **show crypto ca certificates** comando da CLI do AP.

Esse comando permite que você verifique o intervalo de validade do certificado definido no AP. Este é um exemplo:

```
AP00c1.649a.be5c#show crypto ca cert
.........................................
.........................................
.........................................
.............................................
Certificate
Status: Available
Certificate Serial Number (hex): 7D1125A900000002A61A
Certificate Usage: General Purpose
Issuer:
cn=Cisco Manufacturing CA SHA2
o=Cisco
Subject:
Name: AP1G2-00c1649abe5c
e=support@cisco.com
cn=AP1G2-00c1649abe5c
o=Cisco Systems
l=San Jose
st=California
c=US
CRL Distribution Points:
http://www.cisco.com/security/pki/crl/cmca2.crl
Validity Date:
start date: 01:05:37 UTC Mar 24 2016
end date: 01:15:37 UTC Mar 24 2026
Associated Trustpoints: Cisco_IOS_M2_MIC_cert
Storage:
...............................
...................................
.....................................
```

A saída inteira não é listada porque pode haver muitos intervalos de validade associados à saída desse comando. Considere apenas o intervalo de validade especificado pelo Ponto de Confiança Associado: Cisco_IOS_MIC_cert com o nome do AP relevante no campo de nome. Neste exemplo, a saída é `Name: C1200-001563e50c7e`. Esse é o intervalo de validade do certificado real a ser considerado.

- Consulte o bug da Cisco ID CSCuq19142



LAP/WLC MIC ou a expiração da vida útil do SSC causa falha de DTLS: bug da Cisco ID CSCuq19142.

Problema 2: Incompatibilidade no domínio regulamentado

Você verá esta mensagem na saída do **debug capwap events enable** comando:

<#root>

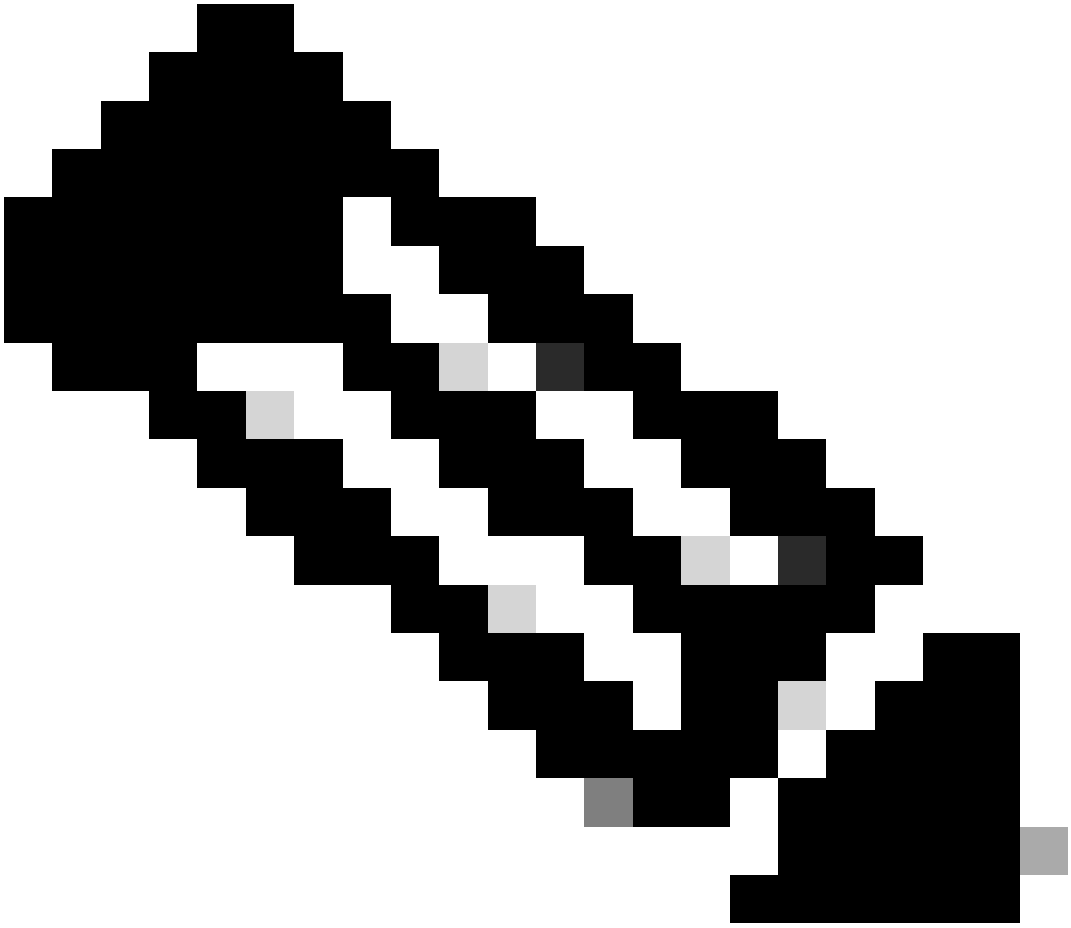
```
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
*spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure
```

***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Setting MTU to1485**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 AP 00:cc:fc:13:e5:e0: Country code is not configure**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Regulatory Domain Mismatch: AP 00:cc:fc:13:e5:e0 no**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Finding DTLS connection to delete for AP (192:168:4**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 Disconnecting DTLS Capwap-Ctrl session 0x1d4df620 f**
***spamApTask7: Jun 28 11:56:49.177: 00:cc:fc:13:e5:e0 acDtlsPlumbControlPlaneKeys: lrad:192.168.47.29(603**

WLC msglog show these messages :

*spamApTask5: Jun 28 11:52:06.536: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7095 00:cc:fc:13:e5:e0: DT
closed forAP 192:168:47:28 (60389), Controller: 10:63:84:78 (5246) Regulatory Domain Mismatch

A mensagem indica claramente que há uma incompatibilidade no domínio regulatório do LAP e do WLC. A WLC suporta vários domínios regulatórios, mas cada domínio regulatório deve ser selecionado antes que um AP possa ingressar a partir desse domínio. Por exemplo, o WLC que usa o domínio regulatório -A somente pode ser usado com APs que usam o domínio regulatório -A (e assim por diante). Ao comprar APs, certifique-se de que eles compartilhem o mesmo domínio regulatório. Somente assim os APs podem se registrar com a WLC.



Observação: os rádios 802.1b/g e 802.11a devem estar no mesmo domínio regulatório para um único AP.

Problema 3: Lista de autorização de AP habilitada na WLC; LAP não está na lista de autorização

Nesses casos, você verá esta mensagem no controlador na saída do comandodebug capwap events enable:

<#root>

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received CAPWAP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
```

```
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST
from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'
Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of
CAPWAP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 Received CAPWAP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce  00:0B:85:33:52:80
rxNonce  00:0B:85:51:5A:E0
Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 CAPWAP Join-Request MTU path from
AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0
Wed Sep 12 17:42:50 2007:
```

spamRadiusProcessResponse: AP Authorization failure

for 00:0b:85:51:5a:e0

Se você usar um LAP que tenha uma porta de console, verá esta mensagem quando emitir o debug capwap client error comando:

```
<#root>
```

```
AP001d.a245.a2fb#
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG: spamHandleJoinTimer: Did not receive the
Join response
*Mar  1 00:00:52.267: LWAPP_CLIENT_ERROR_DEBUG:
```

No more AP manager IP addresses remain.

Isso novamente é uma indicação clara de que o LAP não faz parte da lista de autorização de AP na controladora.

Você pode visualizar o status da lista de autorização de AP com este comando:

<#root>

```
(Cisco Controller) >
```

show auth-list

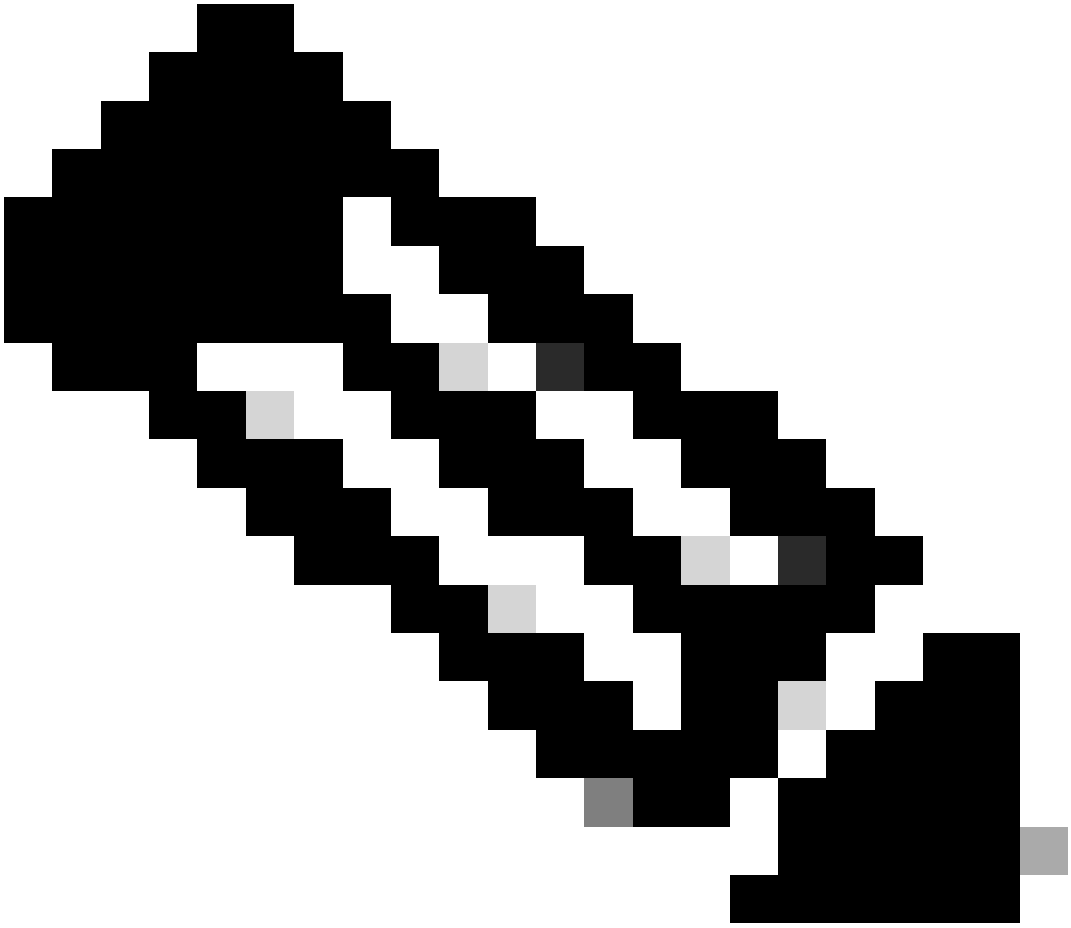
```
Authorize APs against AAA ..... enabled
Allow APs with Self-signed Certificate (SSC) .... disabled
```

Para adicionar um LAP à lista de autorização de AP, use o config auth-list add mic <AP MAC Address> comando. Para obter mais informações sobre como configurar a autorização do LAP, consulte Lightweight Access Point (LAP) Authorization in a Cisco Unified Wireless Network Configuration Example.

Problema 4: Há um certificado ou uma chave pública corrompida no AP

O LAP não se junta a um controlador por causa de um problema de certificado.

Emita os debug capwap errors enable comandos e **debug pm pki enable** . Você vê mensagens que indicam os certificados ou as chaves que estão corrompidos.



Observação: algumas linhas da saída foram movidas para a segunda linha devido a restrições de espaço.

<#root>

```
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 CAPWAP
```

Join Request does not include valid certificate in CERTIFICATE_PAYLOAD
from AP 00:0f:24:a9:52:e0

```
.
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0
 Deleting and removing AP 00:0f:24:a9:52:e0 from fast path
Tue Aug 12 17:36:09 2008: 00:0f:24:a9:52:e0 Unable to free public key for AP
```

Use uma destas duas opções para resolver o problema:

- AP MIC - Solicite uma autorização de devolução de materiais (RMA).
- AP LSC - Provisiona novamente o certificado LSC.

Problema 5: O controlador recebe a mensagem de descoberta de AP na VLAN incorreta (você vê a depuração da mensagem de descoberta, mas não a resposta)

Você verá esta mensagem na saída dodebug capwap events enable comando:

<#root>

Received a Discovery Request with subnet broadcast with wrong AP IP address (A.B.C.D)!

Essa mensagem significa que o controlador recebeu uma solicitação de detecção por um endereço IP de broadcast com um endereço IP de origem que não está em nenhuma sub-rede configurada no controlador. Isso também significa que o controlador é aquele que descarta o pacote.

O problema é que o AP não é o que enviou a solicitação de descoberta ao endereço IP de gerenciamento. O controlador relata uma solicitação de descoberta de broadcast de uma VLAN que não está configurada no controlador. Isso geralmente ocorre quando os troncos permitem VLANs e não as restringem a VLANs sem fio.

Conclua estas etapas para resolver o problema:

- Se o controlador estiver em outra sub-rede, os APs devem ser **preparados** para o endereço IP do controlador ou os APs devem

receber o endereço IP do controlador com o uso de um dos métodos de descoberta.

- O switch está configurado para permitir algumas VLANs que não estão no controlador. Restrinja as VLANs permitidas nos troncos.

Problema 6: O AP não consegue se unir à WLC, o firewall bloqueia as portas necessárias

Se um firewall for usado na rede corporativa, verifique se essas portas estão ativadas no firewall para que o LAP se una e se comunique com a controladora.

Você deve ativar estas portas:

- Ative estas portas UDP para o tráfego CAPWAP:
  - Dados - 5247
  - Controle - 5246
- Ative estas portas UDP para o tráfego de mobilidade:
  - 16666 - 16666
  - 16667 - 16667

- Ative as portas UDP 5246 e 5247 para o tráfego CAPWAP.

- TCP 161 e 162 para o SNMP (para o Wireless Control System [WCS])

Essas portas são opcionais (dependendo de seus requisitos):

- UDP 69 para o TFTP

- TCP 80 e/ou 443 para o HTTP ou o HTTPS para o acesso a GUI

- TCP 23 e/ou 22 para o Telnet ou o SSH para o acesso a CLI

Problema 7: Endereço IP duplicado na rede

Esse é outro problema comum visto quando o AP tenta se unir à WLC. Você pode ver essa mensagem de erro quando o AP tenta juntar-se à controladora.

No more AP manager IP addresses remain

Uma das razões para essa mensagem de erro é quando há um endereço IP duplicado na rede que corresponde ao endereço IP do gerenciador AP. Nesse caso, o LAP mantém as iniciações do ciclo de energia e não pode se unir à controladora.

As depurações mostram que a WLC recebe solicitações de descoberta LWAPP dos APs e transmite uma resposta de descoberta LWAPP aos APs.

Contudo, os WLC não recebem solicitações de junção do LWAPP a partir dos APs.

Para solucionar esse problema, execute ping no gerenciador AP de um host com fio na mesma sub-rede IP que o gerenciador AP. Depois, verifique o cachê ARP. Se um endereço IP duplicado for encontrado, remova o dispositivo com o endereço IP duplicado ou altere o endereço IP no dispositivo para que ele tenha um endereço IP exclusivo na rede.

O AP poderá então juntar-se ao WLC.

Problema 8: LAPs com imagem de malha não podem se unir ao WLC

O Lightweight Access Point não se registra na WLC. O registro exibe esta mensagem de erro:

```
AAA Authentication Failure for UserName:5475xxx8bf9c User
     Type: WLAN USER
```

Isso pode acontecer se o Lightweight Access Point tiver sido enviado com uma imagem de malha e estiver no modo Bridge. Se o LAP foi solicitado com o software de malha nele, você precisa adicioná-lo à lista de autorização de AP. Escolha **Security > AP Policies** e adicione **AP** à Authorization List. O AP deve então se unir, fazer download da imagem do controlador e, em seguida, registrar com o WLC no modo de ponte. Em seguida, você precisa alterar o AP para o modo local. O LAP baixa a imagem, reinicializa e registra de volta na controladora no modo local.

Problema 9: Endereço incorreto do Microsoft DHCP

Os pontos de acesso podem renovar seus endereços IP rapidamente quando é feita uma tentativa de ingressar em uma WLC, o que pode fazer com que os servidores DHCP do Windows marquem esses IPs como BAD_ADDRESS, o que poderia rapidamente esgotar o pool DHCP. Verifique se há mais informações no capítulo Client Roaming do Cisco Wireless Controller Configuration Guide, Release 8.2.

Informações Relacionadas

- **Suporte técnico e downloads da Cisco**

- **Processo de união de AP com Catalyst 9800**

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.