Solucionar problemas de desassociação do ponto de acesso do controlador

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Processo de registro de AP baseado em controlador](#)
[Caso de uso 1](#)
[Caso de uso 2](#)
[Caso de uso 3](#)
[Caso de uso 4](#)

Introduction

Este documento descreve casos de uso para entender o motivo da interrupção do túnel Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) entre Access Points (APs) e a Wireless LAN Controller (WLC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da configuração do AP e do controlador, além do conhecimento básico de roteamento e switching.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Processo de registro de AP baseado em controlador

Os APs passam pelo processo mencionado para se registrarem na controladora:

1. Solicitação de mensagem de descoberta CAPWAP do AP para a WLC.
2. A mensagem de resposta da descoberta da WLC para o AP.
3. O AP escolhe a WLC para se unir com base na resposta CAPWAP recebida.
4. Solicitação de junção enviada ao WLC do AP.
5. A controladora valida o AP e envia a resposta de junção.

Logs capturados no AP quando registrados no WLC:

Press RETURN to get started! Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

Caso de uso 1

1. Os APs são desassociados da WLC e, quando verificados do switch, mostram que o AP não tem IP.

Registros quando consolados ao AP:

Solução:

Trabalhe para corrigir os problemas de acessibilidade para o endereço IP auxiliar configurado na VLAN se o servidor DHCP estiver localizado remotamente. Se o DHCP estiver configurado localmente, verifique se não há nenhum conflito de DHCP. Configure o IP estático no AP:

Faça login no AP e digite estes comandos:

```
capwap ap ip address <ip> <mask>

capwap ap ip default-gateway <ip>
```

Além disso, você pode especificar o endereço IP do controlador:

capwap ap controller ip address

2. Observe que há APs com endereços IP, mas a falha na comunicação com a WLC pode ser uma falha na resolução do IP da controladora.

Logs do AP com um problema em que a resolução do Sistema de Nome de Domínio (DNS) falhou:

```
<Date & time>  %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER.local doamin

Not in Bound state.
```

Solução:

Verifique a acessibilidade do servidor DNS interno, se aceitável, certifique-se de que os endereços IP do controlador enviados por DHCP estejam acessíveis.

Correção de falhas: Configure o controlador manualmente no AP.

```
"capwap ap {primary-base | secondary-base | tertiary-base}controller-name controller-ip-address"
```

3. Você vê que o AP está registrado no controlador e ainda não vê nenhum broadcast do Service Set Identifier (SSID) necessário.

```
(4402-d) >config wlan apgroup interface-mapping add <ap group name> <wlandi> <interfacename>
```

Solução:
Adicione a LAN sem fio (WLAN) no grupo AP.

Caso de uso 2

Observe que o AP não é visto no vizinho do Cisco Discovery Protocol (CDP) do switch, e o switch conectado ao AP está em um estado desativado por erro.

Logs capturados do Switch:

Dec 9 08:42:35.836 UTC: RSTP(10): sending BPDU out Te3/0/47STP: pak->vlan_id: 10 Dec 9 08:42:35.836 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable stateSTP: pak->vlan_id: 1 Dec 9 09:47:32.651 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD Dec 9 09:47:33.651 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted Dec 9 09:47:53.545 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state Dec 9 09:48:10.955 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD Dec 9 09:48:11.955 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted Dec 9 09:48:32.114 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state

Solução:
O AP não envia o protetor da Bridge Protocol Data Unit (BPDU) sob nenhuma circunstância, isso é um problema do lado do switch. Mova o AP para outra porta livre e replique a configuração da interface juntamente com as verificações físicas necessárias.

Caso de uso 3

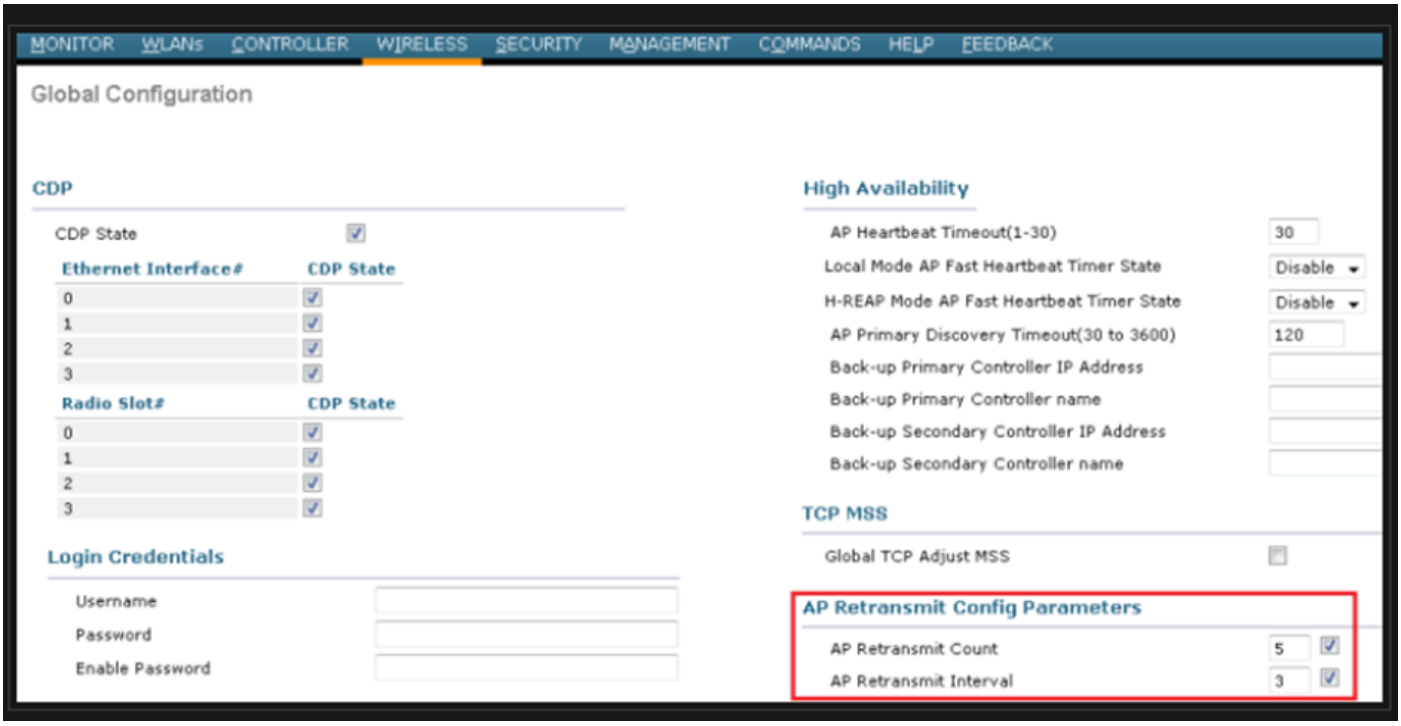
Na configuração do escritório remoto, você frequentemente vê o rompimento do túnel CAPWAP aleatoriamente entre APs e controlador, e o parâmetro mais importante a ser verificado é o intervalo de retransmissão e repetição.

O intervalo de retransmissão do AP e o intervalo de repetição podem ser configurados tanto no nível global quanto no nível do AP. Uma configuração global aplica esses parâmetros de configuração a todos os APs. Ou seja, o intervalo de retransmissão e a contagem de repetições são uniformes para todos os APs.

Registros problemáticos do WLC:

*spamApTask6: Jun 01 17:17:55.426: %LWAPP-3-AP_DEL: spam_lrad.c:6088 1c:d1:e0:43:1d:20: Entry deleted for AP: 10.209.36.5 (5256) reason : AP Message Timeout. *spamApTask6: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1d:20) event (Capwap_configuration_update_request) and state (Capwap_dtls_teardown) combination -Traceback: 0xe69bba3a5f 0xe69b9b9446 0xe69bdc5e3b 0xe69b8f238c 0xe69bbaf33b 0xe69cc8041b 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d *spamReceiveTask: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1d:20) event (Capwap_configuration_update_request) and state (Capwap_dtls_teardown) combination -Traceback: 0xe69bba3a5f 0xe69b981950 0xe69b76dd5c 0xe69cc757c2 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d *spamApTask5: Jun 01 17:17:55.424: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7521 1c:d1:e0:43:1d:20: DTLS connection closed forAP 10:209:36:5 (5256), Controller: 10:176:92:53 (5246) AP Message Timeout *spamApTask5: Jun 01 17:17:55.423: %CAPWAP-3-MAX_RETRANSMISSIONS_REACHED: capwap_ac_sm.c:8073 Max retransmissions reached on AP(1c:d1:e0:43:1d:20),message (CAPWAP_CONFIGURATION_UPDATE_REQUEST),number of pending messages(2)

Solução: se o problema ocorrer em todos os locais, aumente o **Retransmit count** e **Retransmit interval** em configuração global sem fio. Opção para aumentar os valores quando o problema é para todos os APs.



Opção para alterar os parâmetros de configuração de retransmissão do AP em Configuração global

Se o problema for específico de um local remoto, um aumento na **Retransmit count** e **Retransmit interval** em um AP específico corrige o problema.

Opção para alterar o parâmetro de configuração de retransmissão de AP em um AP específico

Caso de uso 4

O AP se desassocia completamente da WLC e não pode reingressar na controladora; isso pode estar relacionado aos certificados digitais.

Alguns fatos rápidos sobre certificados de dispositivos em termos de WLCs e APs da Cisco:

- Cada dispositivo da Cisco vem com um certificado padrão com uma validade de 10 anos.
- Este certificado é usado para realizar a autenticação entre o Cisco WLC e o AP.
- Com a ajuda dos certificados AP e WLC, estabeleça um túnel seguro de Datagram Transport Layer Security (DTLS).

Encontrados dois tipos de problemas relacionados a certificados:

Problema 1: AP mais antigo (não quer entrar na WLC).

O console para o AP ajuda a determinar o problema e os registros são como se segue:

*Sep 13 18:26:24.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.1.1 peer_port: 5246 *Sep 13 18:26:24.000: %CAPWAP-5-CHANGED: CAPWAP changed state to *Sep 13 18:26:24.099: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The certificate (SN: XXXXXXXXXXXXX) has expired. Validity period ended on 19:56:24 UTC Aug 12 2018 *Sep 13 18:26:24.099: %LWAPP-3-CLIENTERRORLOG: Peer certificate verification failed *Sep 13 18:26:24.099: %CAPWAP-3-ERRORLOG: Certificate verification failed!

Problema 2: O AP mais recente não quer se unir a uma WLC mais antiga.
O console para o AP fornece um erro que poderia ser semelhante a este:

[*09/09/2019 04:55:26.3299] CAPWAP State: DTLS Teardown [*09/09/2019 04:55:30.9385] CAPWAP State: Discovery [*09/09/2019 04:55:30.9385] Did not get log server settings from DHCP. [*09/09/2019 04:55:41.0000] CAPWAP State: DTLS Setup [*09/09/2019 04:55:41.3399] Bad certificate alert received from peer. [*09/09/2019 04:55:41.3399] DTLS: Received packet caused DTLS to close connection

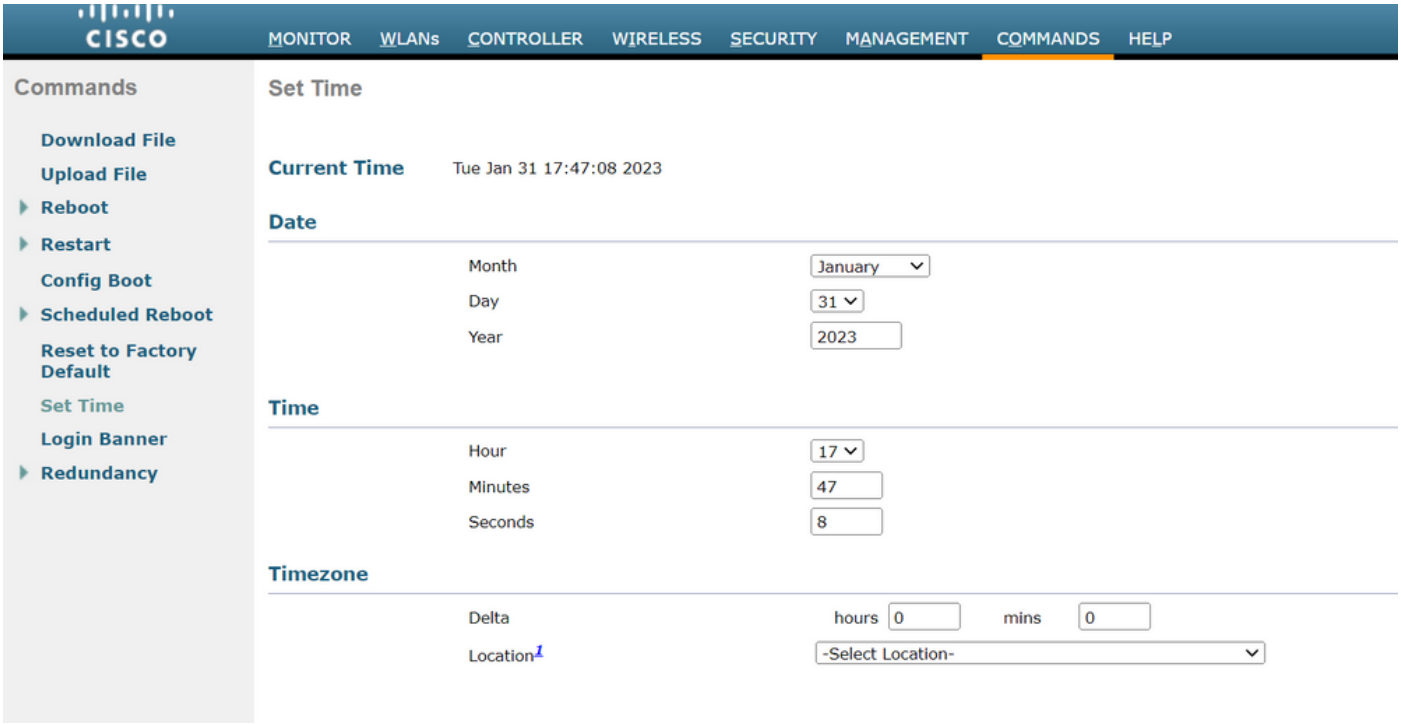
Solução:

1. O NTP desabilita e define o horário manualmente através do CLI:

(Cisco Controller)> config time ntp delete 1 (Cisco Controller)> config time manual 09/30/18 11:30:00

2. O NTP desabilita e define o horário manualmente por meio da GUI:

Navegue até **Controller > NTP > Server > Commands > Set Time** para remover os servidores NTP listados.



Local para definir o horário manualmente na GUI

2. Desative o MIC (Manufaturer Installed Certificate) na controladora. Esse comando é aceito apenas nas versões mais recentes.

```
(Cisco Controller)> config ap cert-expiry-ignore mic enable
```

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.