Solucionar problemas de desasociación del punto de acceso del controlador

Contenido

Introducción

En este documento se describen casos prácticos para comprender la razón de la interrupción del túnel Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) entre los puntos de acceso (AP) y el Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la configuración del controlador y del AP, junto con conocimientos básicos de ruteo y switching.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Proceso de registro de AP basado en controlador

Los AP pasan por el proceso mencionado para registrarse con el controlador:

1. Solicitud de mensaje de detección CAPWAP al WLC desde el AP.
2. El mensaje de respuesta de detección del WLC al AP.
3. AP elige el WLC para unirse basado en la respuesta CAPWAP recibida.
4. Solicitud de unión enviada al WLC desde el AP.
5. El controlador valida el AP y envía la respuesta de unión.

Registros capturados en el AP cuando se registra con el WLC:

Press RETURN to get started!

Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

%CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY

status of voice_diag_test from WLC is false

%SSH-5-ENABLED: SSH 2.0 has been enabled

Logging LWAPP message to 255.255.255.255.

%CDP_PD-4-POWER_OK: 15.4 W power - NEGOTIATED inline power source

%LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up

%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to up

%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - CLI initiated

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up Translating "CISCO-LWAPP-CONTROLLER"...dom

%CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip:

peer_port: 5246

%CAPWAP-5-CHANGED: CAPWAP changed state to

%CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip:

peer_port: 5246

%CAPWAP-5-SENDJOIN: sending Join Request to

%CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

%CAPWAP-5-CHANGED: CAPWAP changed state to CFG

%LWAPP-3-CLIENTERRORLOG: Operator changed mode for 802.11g. Rebooting.

%LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down

%SYS-5-RELOAD: Reload requested by CAPWAP CLIENT. Reload Reason: Operator changed mode for 802.11g.

%LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down IOS Bootloader - Starting system.

Caso práctico 1

1. Los AP se desasocian del WLC y cuando se verifica del switch, muestra que el AP no tiene IP.

Registros cuando se consuelan en el AP:

LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up

%CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!

Solución:

Trabaje para solucionar los problemas de disponibilidad en la dirección de ayudante IP configurada bajo la VLAN si el servidor DHCP está ubicado remotamente. Si el DHCP está configurado localmente, asegúrese de que no haya conflicto DHCP. Configure la IP estática en el AP:

Inicie sesión en AP y escriba estos comandos:

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

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

Además, puede especificar la dirección IP del controlador:

capwap ap controller ip address

2. Observe que hay AP con las direcciones IP, pero la falta de comunicación con el WLC podría ser una falla de la resolución al IP del controlador.

Registros del punto de acceso con un problema en el que no se pudo resolver el sistema de nombres de dominio (DNS):

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

Not in Bound state.
```

Solución:

Compruebe la disponibilidad del servidor DNS interno; si es aceptable, asegúrese de que las direcciones IP del controlador que se envían a través de DHCP son accesibles.

Break-fix: Configure el controlador manualmente en el AP.

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

3. Verá que el AP está registrado en el controlador y aún no verá difusión del identificador de conjunto de servicios (SSID) requerido.

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

Solución:
Agregue la LAN inalámbrica (WLAN) en el grupo de puntos de acceso.

Caso práctico 2

Observe que el AP no se ve en el vecino del Cisco Discovery Protocol (CDP) del switch y que el switch conectado al AP está en un estado de inhabilitación por error.

Registros capturados desde el 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

Solución:
El AP no envía la protección de la Unidad de datos de protocolo de puente (BPDU) bajo ninguna circunstancia, esto es un problema del lado del switch. Mueva el AP a otro puerto libre y replique la configuración de la interfaz junto con las verificaciones físicas necesarias.

Caso práctico 3

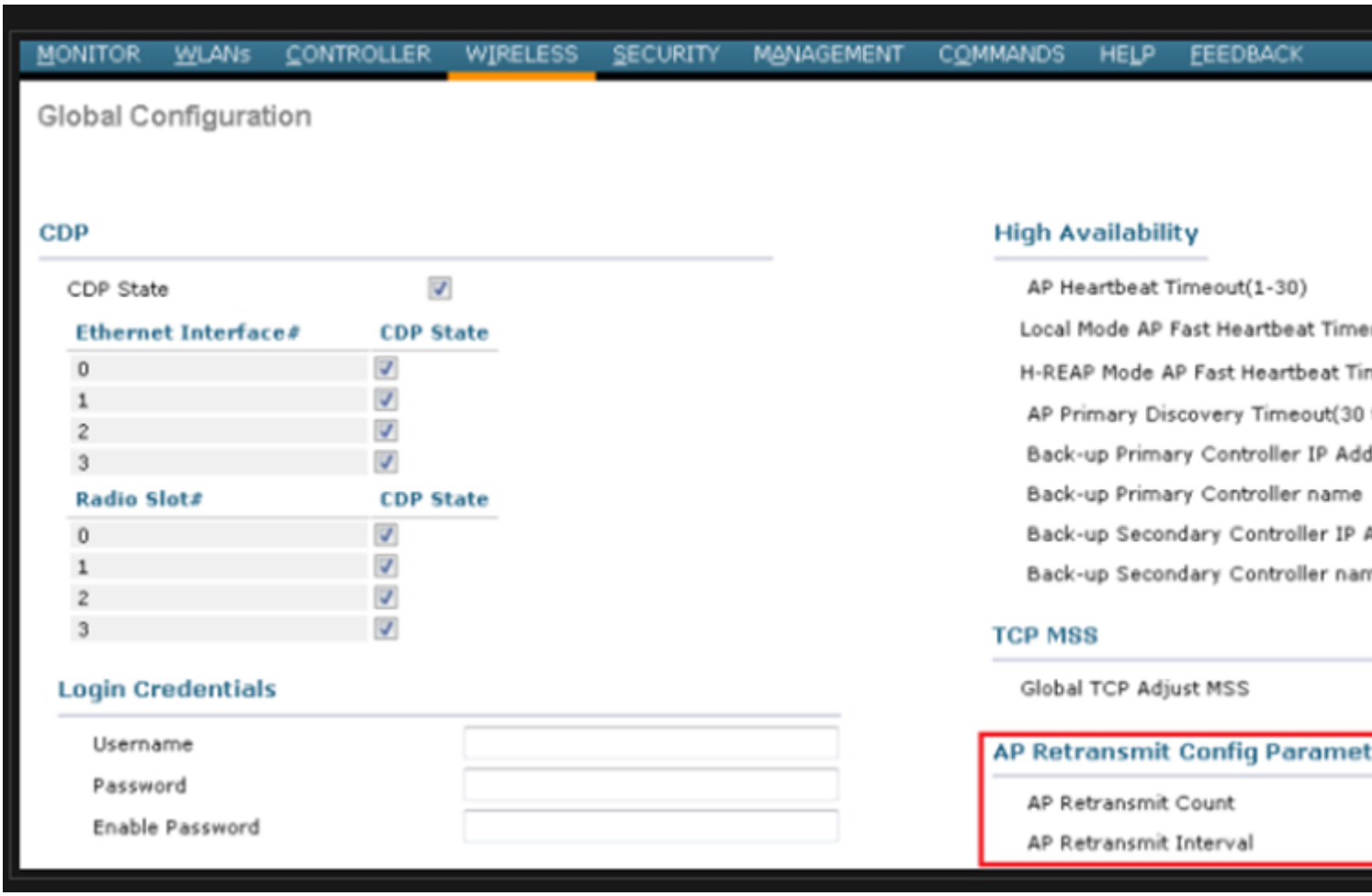
En la configuración de la oficina remota, a menudo se ve el túnel CAPWAP desmontarse aleatoriamente entre los AP y el controlador y el parámetro más importante para verificar son la retransmisión y el intervalo de reintento.

El intervalo de retransmisión de AP y el intervalo de reintento se pueden configurar tanto en el nivel global como en el nivel de AP. Una configuración global aplica estos parámetros de configuración a todos los AP. Es decir, el intervalo de retransmisión y el conteo de reintentos es uniforme para todos los AP.

Registros problemáticos del WLC:

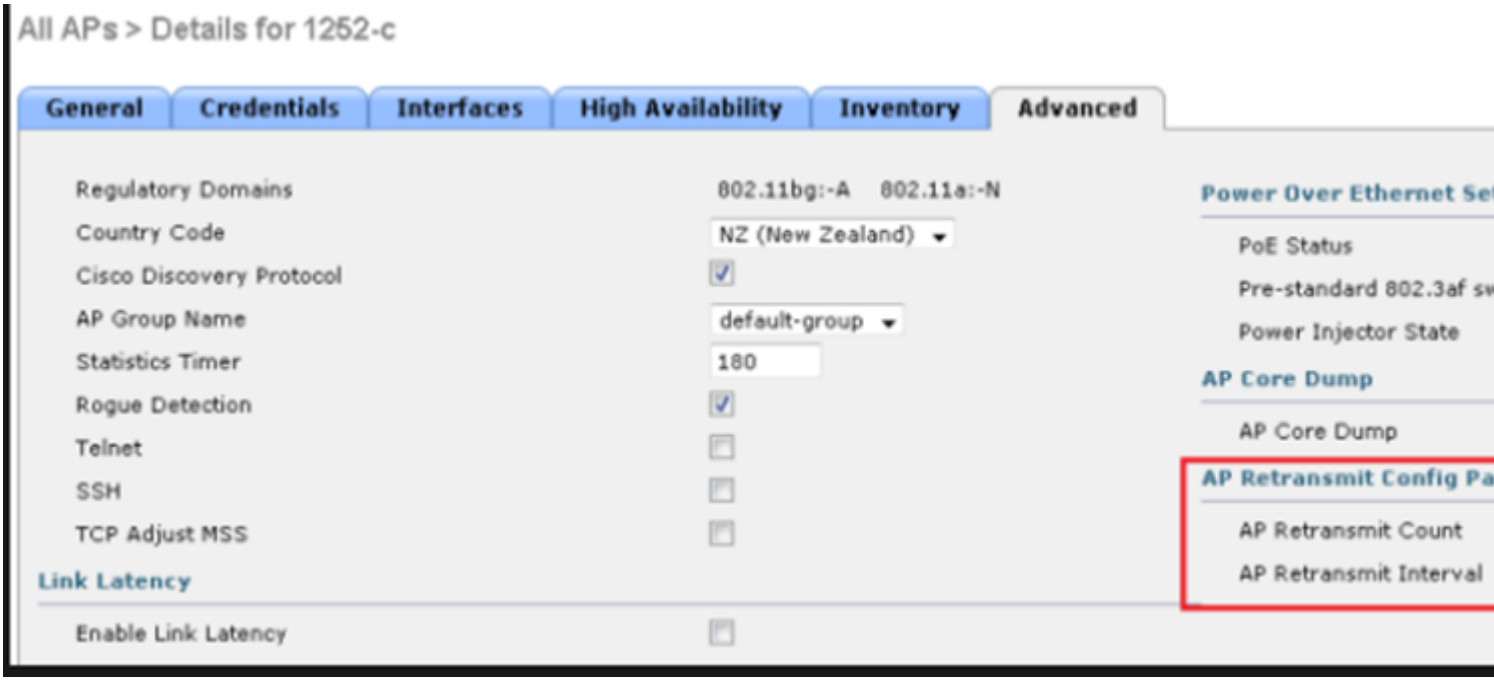
*spamApTask6: Jun 01 17:17:55.426: %LWAPP-3-AP_DEL: spam_lrad.c:6088 1c:d1:e0:43:1d:20: Entry deleted for AP: 10.209.36.5 (5256) reason : AP

Solución: si el problema se produce en todos los sitios, aumente el **Retransmit count** y **Retransmit interval** en configuración global inalámbrica. Opción para aumentar los valores cuando el problema es para todos los AP.



Opción para cambiar los parámetros de configuración de retransmisión de AP bajo la configuración global

Si el problema es específico de un sitio remoto, se producirá un aumento en **Retransmit count** y **Retransmit interval** en un AP determinado soluciona el problema.



Opción para cambiar el parámetro de configuración de retransmisión de AP bajo un AP específico

Caso práctico 4

El AP se desasocia completamente del WLC y no puede volver a unirse al controlador esto podría estar relac

- Este certificado se utiliza para realizar la autenticación entre el WLC y el AP de Cisco.
- Con la ayuda de los certificados AP y WLC establecen un túnel seguro de la seguridad de la capa de transporte del datagrama (DTLS).

Se encontraron dos tipos de problemas relacionados con los certificados:

Problema 1: AP más antiguo (no quiere unirse al WLC).

La consola al AP ayuda a determinar el problema y los registros se ven de la siguiente manera:

```
*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: XXXXXXXXXXXXXX) 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: El AP más nuevo no quiere unirse a un WLC más antiguo.
La consola al AP da un error que podría verse así:

```
[*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
```

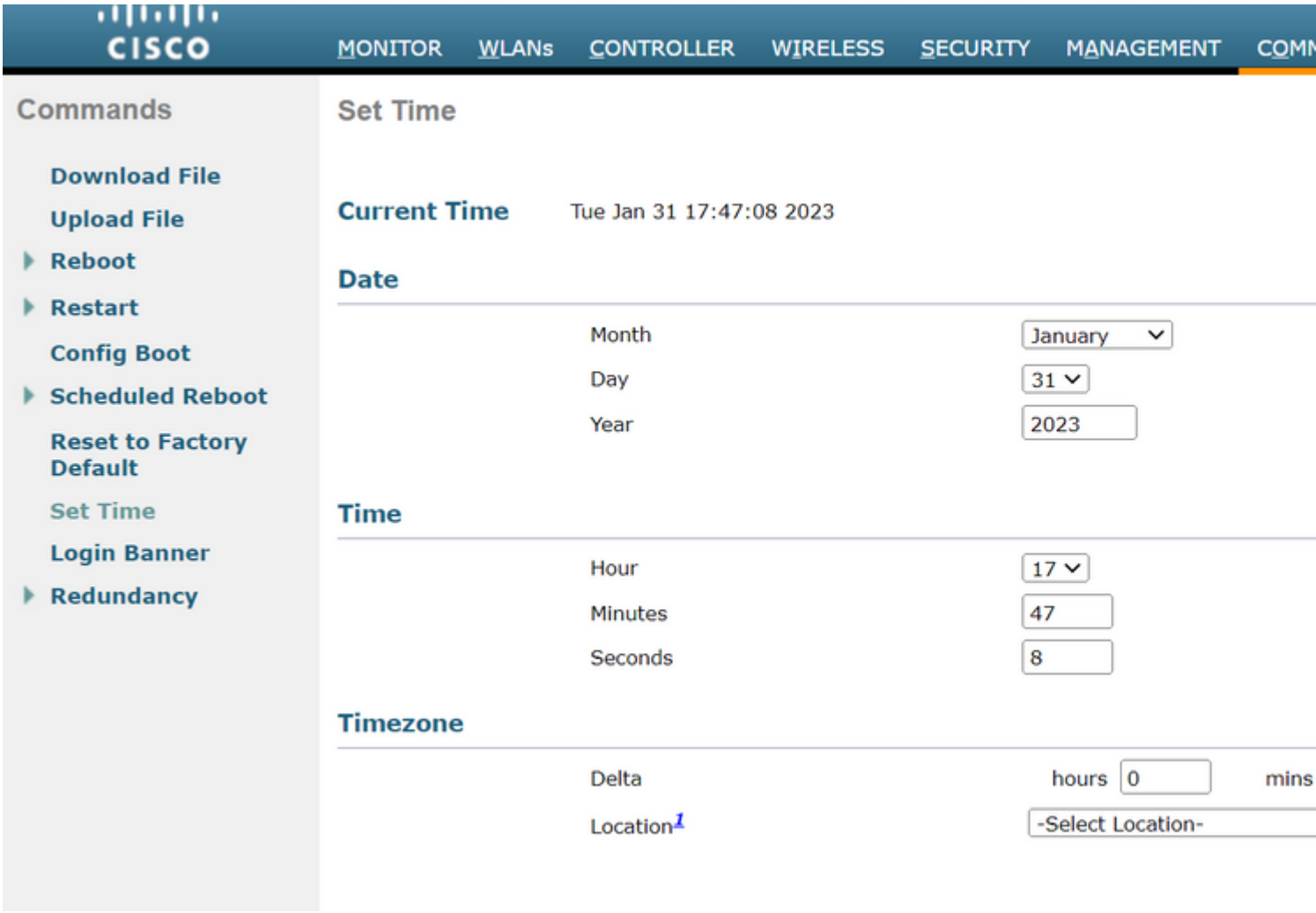
Solución:

1. NTP inhabilita y establece el tiempo manualmente a través de CLI:

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

2. NTP inhabilita y establece el tiempo manualmente a través de la GUI:

Desplácese hasta **Controller > NTP > Server > Commands > Set Time** para quitar los servidores NTP enumerados.



Ubicación para establecer la hora manualmente en la GUI

2. Inhabilite el certificado instalado por el fabricante (MIC) en el controlador. Este comando sólo se acepta en las versiones más recientes.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).