Risoluzione dei problemi di dissociazione del punto di accesso dal controller

Sommario

Introduzione

In questo documento vengono descritti gli use case per comprendere le interruzioni del tunnel CAPWAP/LWAPP tra i punti di accesso (Access Point) e il controller WLC (Wireless LAN Controller).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di punti di accesso (AP) e controller WLC
- Routing e switching.
- Controllo e provisioning dei punti di accesso wireless (CAPWAP)
- Protocollo LWAPP (Lightweight Access Point Protocol)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento vengono descritti gli use case per comprendere il motivo per cui controllare e fornire punti di accesso wireless (CAPWAP)/Lightweight Access Point Protocol (LWAPP) si è verificato un errore di interruzione del tunnel tra i punti di accesso (AP) e il controller WLC.

Processo di registrazione dei punti di accesso basati su controller

Gli access point eseguono la procedura descritta di seguito per registrarsi presso il controller:

1. Richiesta di messaggio di individuazione CAPWAP al WLC dagli access point.
2. Messaggio di risposta di individuazione dal WLC agli access point.
3. Gli access point scelgono il WLC da unire in base alla risposta CAPWAP ricevuta.
4. Richiesta di aggiunta inviata al WLC dagli access point.
5. Il controller convalida gli access point e invia la risposta join.

Registri acquisiti sugli access point quando registrati sul WLC:

Press RETURN to get started!

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

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY

<Date & time> status of voice_diag_test from WLC is false

<Date & time> %SSH-5-ENABLED: SSH 2.0 has been enabled

<Date & time> Logging LWAPP message to 255.255.255.255.

<Date & time> %CDP_PD-4-POWER_OK: 15.4 W power - NEGOTIATED inline power source

<Date & time> %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up

<Date & time> %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

<Date & time> %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to up

<Date & time> %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - CLI initiated

<Date & time> %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up

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

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

<Date & time> %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: <controller IP> peer_port: 5246

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to

<Date & time> %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: <controller IP> peer_port: 5246

<Date & time> %CAPWAP-5-SENDJOIN: sending Join Request to <controller IP>

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to CFG

<Date & time> %LWAPP-3-CLIENTERRORLOG: Operator changed mode for 802.11g. Rebooting.

<Date & time> %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down

<Date & time> %SYS-5-RELOAD: Reload requested by CAPWAP CLIENT. Reload Reason: Operator changed mode for 802.11g.

<Date & time> %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down

IOS Bootloader - Starting system.

Caso di utilizzo 1

1. L'associazione tra i punti di accesso e il WLC viene annullata e, una volta verificati dallo switch, viene mostrato che i punti di accesso non dispongono di IP.

Registra quando viene consolato negli access point:

<Date & time> LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up

<Date & time> %CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!

Soluzione:

Risolvere i problemi di raggiungibilità dell'indirizzo dell'helper IP configurato nella VLAN se il server DHCP si trova in remoto. Se DHCP è configurato localmente, verificare che non vi siano conflitti DHCP. Configurare l'IP statico sugli access point:

Accedere agli access point e digitare i seguenti comandi:

capwap ap ip address <ip> <mask>

capwap ap ip default-gateway <ip>

Inoltre, è possibile specificare l'indirizzo IP del controller:

capwap ap controller ip address <ip>

2. Si noti che esistono access point con indirizzi IP, ma la mancata comunicazione con il WLC potrebbe essere un errore di risoluzione per il controller IP.

Registri dai punti di accesso con un problema in cui la risoluzione DNS (Domain Name System) non è riuscita:

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

Not in Bound state.

Soluzione:

Verificare la raggiungibilità del server DNS interno. Se accettabile, verificare che gli indirizzi IP dei controller inviati tramite DHCP siano raggiungibili.

Break-fix: configurare manualmente il controller sugli access point.

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

3. Si vede che gli access point sono registrati sul controller e che ancora non si vede alcuna trasmissione del necessario SSID (Service Set Identifier).

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

Soluzione:
Aggiungere la rete LAN wireless (WLAN) nel gruppo di access point.

Caso di utilizzo 2

Si noti che i punti di accesso non vengono visualizzati sul router adiacente del protocollo Cisco Discovery Protocol (CDP) dello switch e che lo switch connesso ai punti di accesso è in stato err-disabled.

Registri acquisiti dallo 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

Soluzione:
I punti di accesso non inviano il dispositivo di protezione BDPU (Bridge Protocol Data Unit) in nessuna circostanza; si tratta di un problema che interessa lo switch. Spostare gli access point su un'altra porta libera e replicare la configurazione dell'interfaccia insieme ai controlli fisici

necessari.

Caso di utilizzo 3

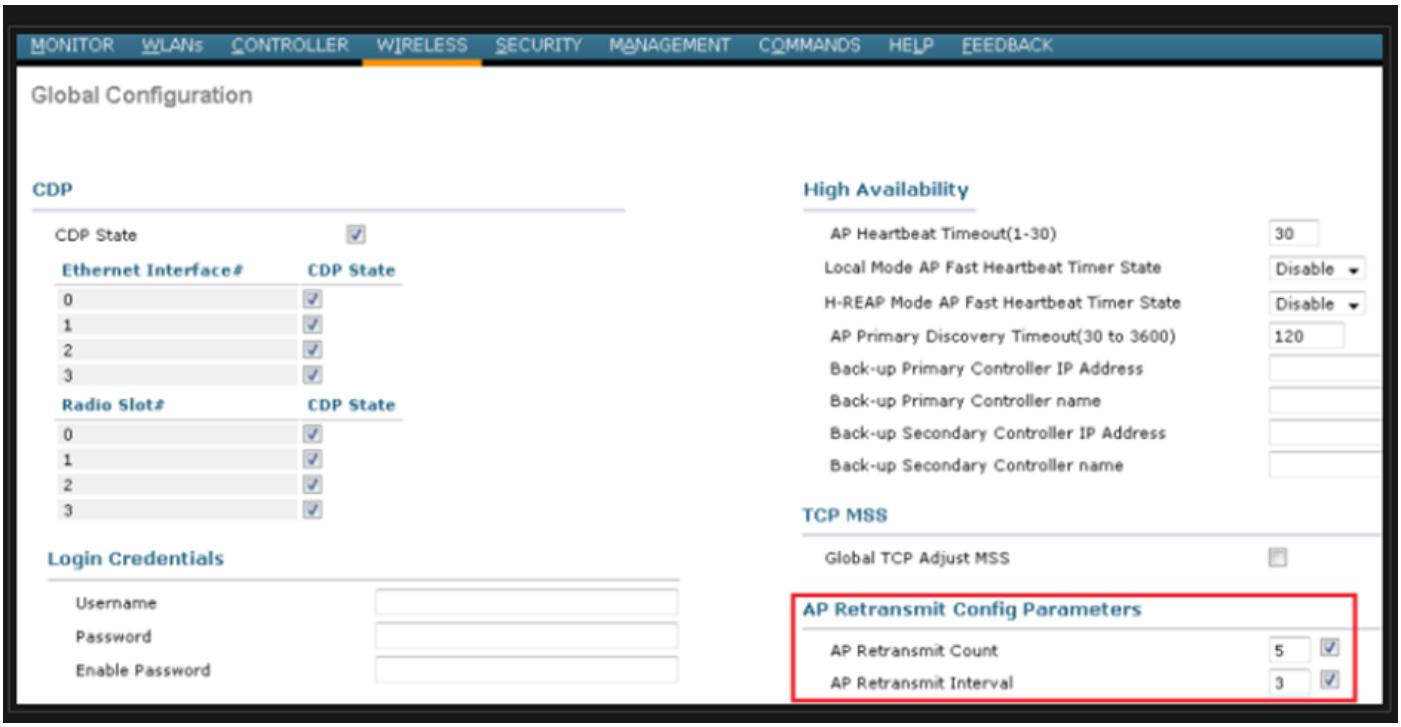
Nella configurazione degli uffici remoti, spesso il tunnel CAPWAP viene eliminato in modo casuale tra i punti di accesso e il controller e il parametro più importante da verificare è l'intervallo tra i tentativi di trasmissione e quelli successivi.

L'intervallo di ritrasmissione e l'intervallo tra tentativi dei punti di accesso possono essere configurati sia a livello globale che a livello dei punti di accesso. Una configurazione globale applica questi parametri di configurazione a tutti gli access point. In altri termini, l'intervallo di ritrasmissione e il numero di tentativi sono uniformi per tutti gli access point.

Registri con problemi dal 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

Soluzione: se il problema riguarda tutti i siti, aumentare il numero **Retransmit count** e **Retransmit interval** nella configurazione globale wireless. Opzione per aumentare i valori quando il problema riguarda tutti gli access point.



Opzione per la modifica dei parametri di configurazione della ritrasmissione AP nella configurazione globale

Se il problema è specifico di un sito remoto, l'aumento di **Retransmit count** e **Retransmit interval** su uno specifico access point risolve il problema.

Opzione per modificare il parametro di configurazione della ritrasmissione AP in un punto di accesso specifico

Caso di utilizzo 4

Gli AP vengono completamente dissociati dal WLC e non possono rientrare nel controller perché ciò potrebbe essere correlato ai certificati digitali.

Ecco alcune informazioni sui certificati dei dispositivi in termini di WLC e AP Cisco:

- Tutti i dispositivi forniti da Cisco sono dotati di un certificato per impostazione predefinita con una validità di 10 anni.
- Questo certificato è usato per eseguire l'autenticazione tra il WLC di Cisco e gli access point.
- Con l'aiuto dei certificati AP e WLC, stabilire un tunnel DTLS (Datagram Transport Layer Security) sicuro.

Sono stati rilevati due tipi di problemi relativi ai certificati:

Problema 1: access point precedenti (non desidera unirsi al WLC).

La console agli access point aiuta a determinare il problema e i registri hanno il seguente aspetto:

*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: %CAPW

Problema 2: gli access point più recenti non vogliono unirsi a un WLC precedente.
La console sugli access point restituisce un errore che potrebbe avere il seguente aspetto:

[*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] D

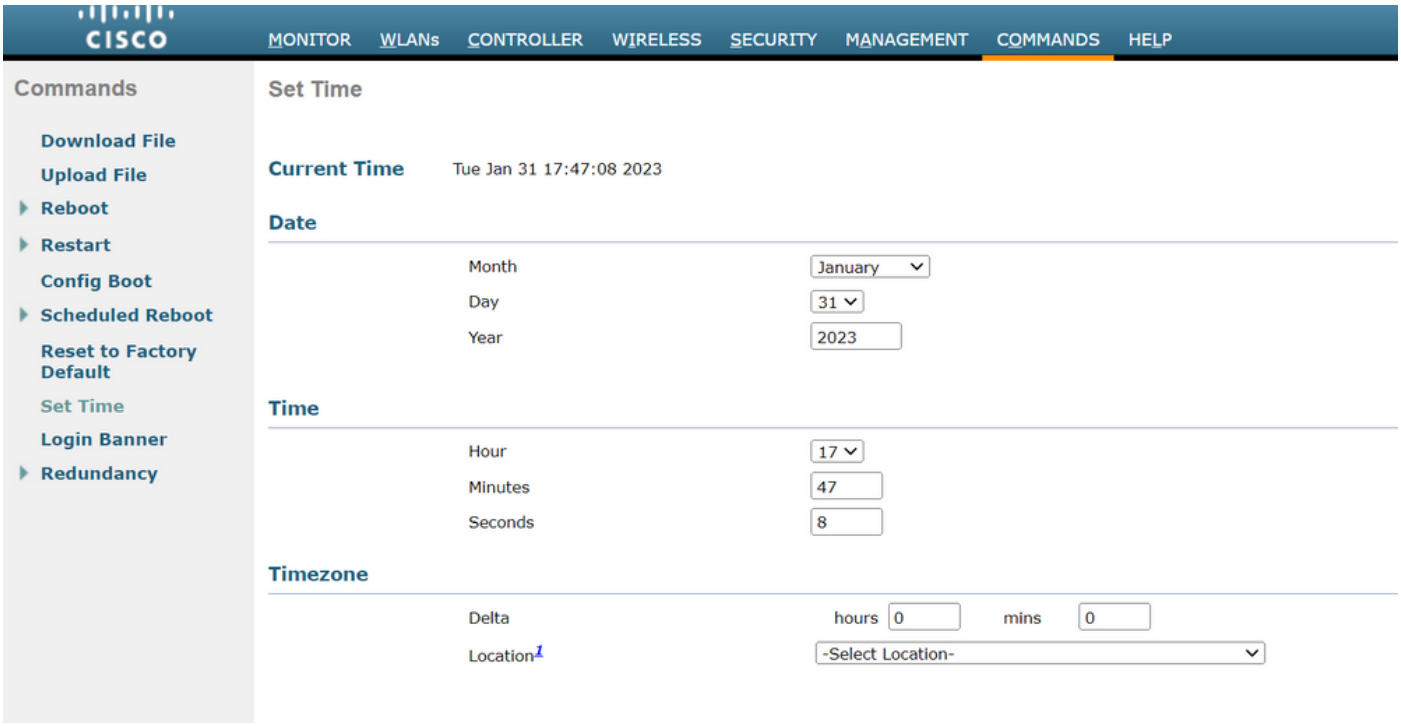
Soluzione:

1. Il protocollo NTP disabilita e imposta manualmente l'ora tramite la CLI:

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

2. Il protocollo NTP disabilita e imposta manualmente l'ora tramite GUI:

Passare a **Controller > NTP > Server > Commands > Set Time** per rimuovere i server NTP elencati.



Posizione per impostare manualmente l'ora sulla GUI

2. Disabilitare il certificato di installazione produttore (MIC) sul controller. Questo comando è accettato solo nelle versioni più recenti.

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

Informazioni correlate

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).