排除接入点与控制器的取消关联故障

目录

简介

本文档介绍使用案例，以了解无线接入点(AP)与无线局域网控制器(WLC)之间无线接入点的控制和调配(CAPWAP)/轻量接入点协议(LWAPP)隧道中断的原因。

先决条件

要求

Cisco建议您具备AP和控制器配置知识以及路由和交换基础知识。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

基于控制器的AP注册流程

AP通过上述过程向控制器注册：

1. 从AP向WLC发出CAPWAP发现消息请求。
2. 从WLC到AP的发现响应消息。
3. AP根据收到的CAPWAP响应选择要加入的WLC。
4. 从AP发送到WLC的加入请求。
5. 控制器验证AP并发送加入响应。

向WLC注册时在AP上捕获的日志：

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"...don

%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.

使用案例1

1. AP与WLC取消关联，从交换机验证后，会显示AP没有IP。

当控制台连接到AP时登录：

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 !!

解决方案：

如果DHCP服务器位于远程，请修复在VLAN下配置的IP帮助地址的可达性问题。如果DHCP是在本地配置的，请确保没有DHCP冲突。在AP上配置静态IP:

登录到AP并键入以下命令：

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

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

此外，还可以指定控制器IP地址：

```
capwap ap controller ip address
```

2.请注意，存在具有IP地址的AP，但无法与WLC通信可能是控制器IP的分辨率故障。

来自AP的日志存在域名系统(DNS)解析失败的问题：

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

Not in Bound state.
```

解决方案：

检查内部DNS服务器的可达性（如果可接受），确保通过DHCP推送的控制器IP地址可访问。

中断修复：在AP上手动配置控制器。

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

3.您看到AP已在控制器上注册，并且仍然没有看到所需的服务集标识符(SSID)广播。

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

解决方案：
请在AP组下添加无线局域网(WLAN)。

使用案例2

请注意，交换机的Cisco发现协议(CDP)邻居上未显示AP，并且AP连接的交换机处于错误禁用状态。

从交换机捕获的日志：

```
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
```

解决方案：
AP在任何情况下都不会发送网桥协议数据单元(BPDU)防护，这是交换机端的问题。将AP移动到另一个空闲端口，并复制接口配置以及必要的物理检查。

使用案例3

在远程办公室设置中，您经常会看到AP和控制器之间的CAPWAP隧道随机中断，要检查的最重要

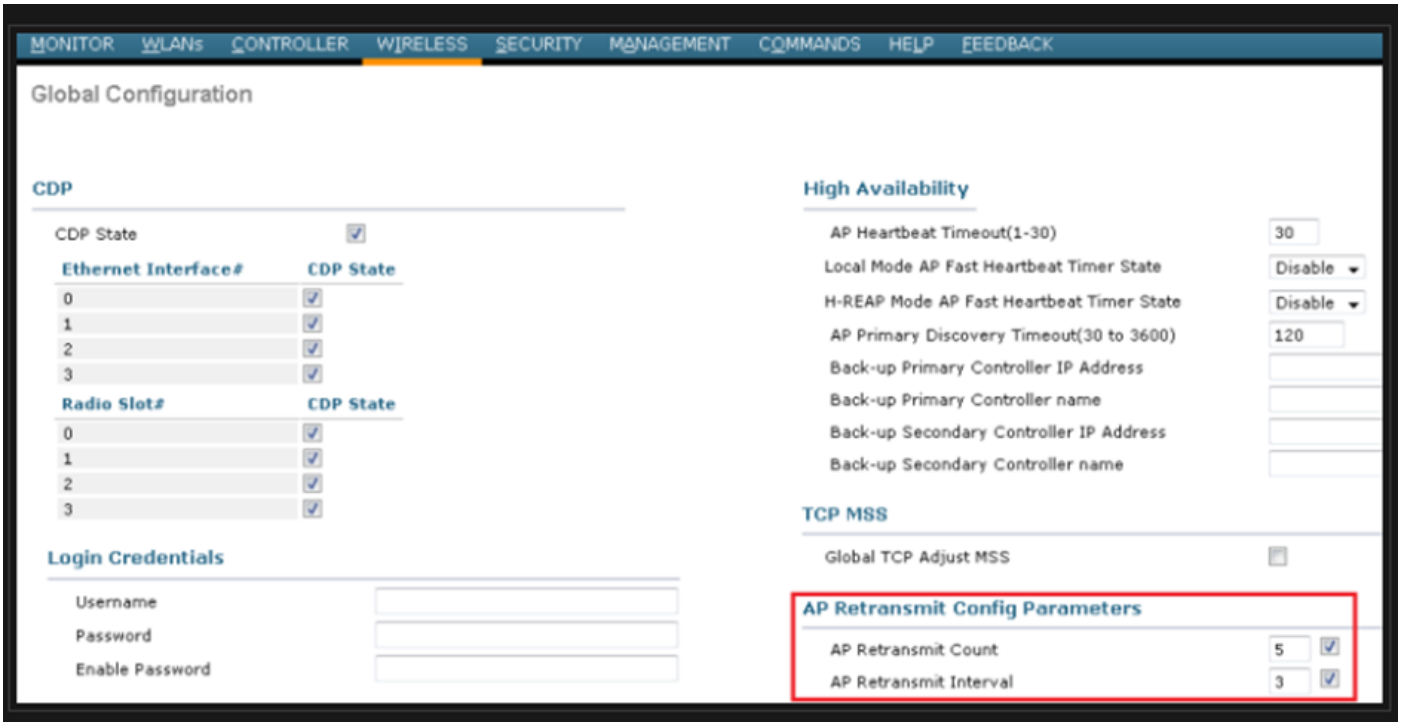
参数是重新传输和重试间隔。

AP重传间隔和重试间隔可在全局级别和AP级别配置。全局配置将这些配置参数应用于所有AP。也就是说，所有AP的重传间隔和重试计数是统一的。

来自WLC的问题日志：

*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

解决方案：如果问题涉及所有站点，则增加 **Retransmit count** 和 **Retransmit interval** 在wireless Global configuration下。选项可在所有AP出现问题时增加值。



用于更改Global configuration下的AP重新传输配置参数的选项

如果问题仅针对一个远程站点，则增加 **Retransmit count** 和 **Retransmit interval** 在特定AP上修复此问题。

使用案例4

AP与WLC完全取消关联，无法重新加入控制器，这可能与数字证书相关。

有关思科WLC和AP的设备证书的一些简略说明：

- 默认情况下，思科提供的每个设备都附带一个有效期为10年的证书。
- 此证书用于在Cisco WLC和AP之间执行身份验证。
- 在证书的帮助下，AP和WLC建立安全的数据报传输层安全(DTLS)隧道。

遇到两种与证书相关的问题：

问题1：旧AP（不想加入WLC）。

通过控制台连接到AP有助于确定问题，日志如下所示：

```
*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!
```

问题2：较新的AP不想加入较旧的WLC。
AP的控制台显示的错误可能如下所示：

```
[*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
```

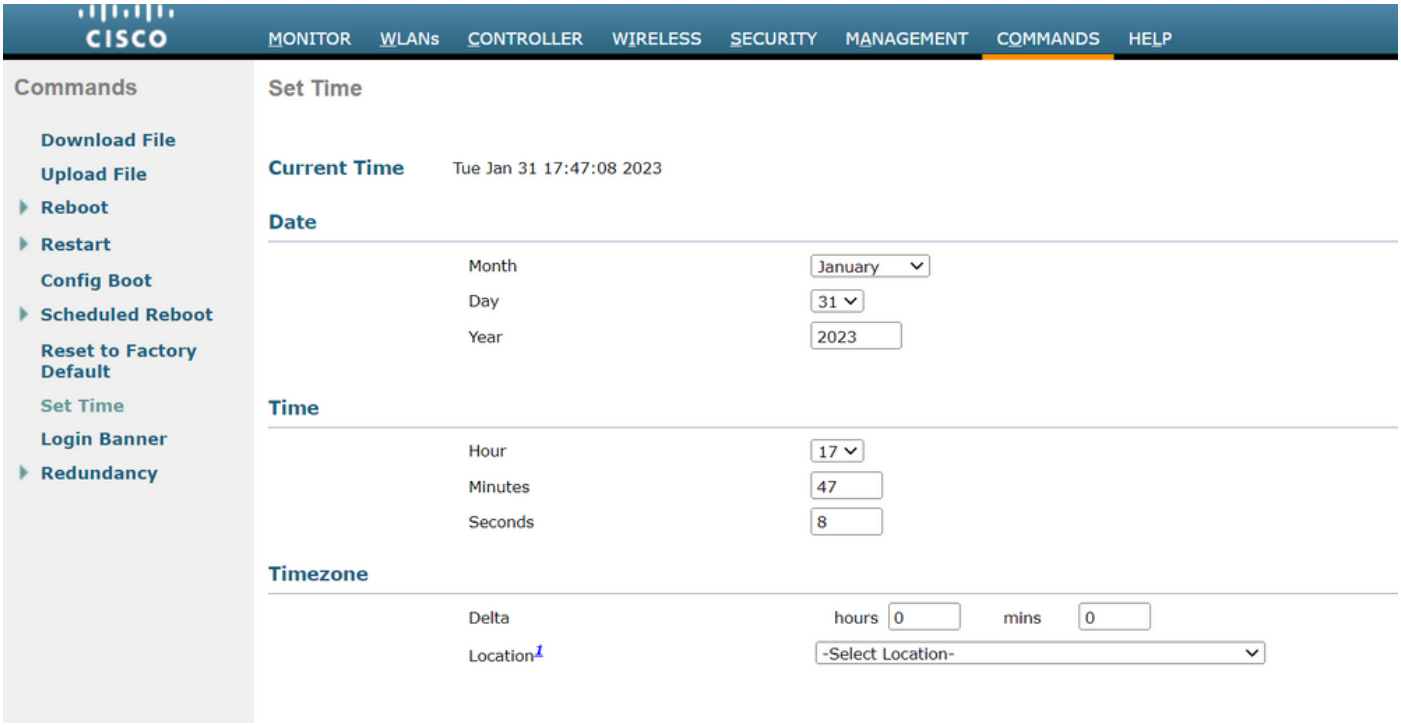
解决方案：

1. NTP通过CLI禁用和手动设置时间：

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

2. NTP通过GUI禁用和手动设置时间：

导航至 **Controller > NTP > Server > Commands > Set Time** 以删除列出的NTP服务器。



在GUI上手动设置时间的位置

2.禁用控制器上的制造商安装证书(MIC)。此命令仅在最新版本上被接受。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。