

在WAP125或WAP581接入點上配置資料包捕獲

目標

封包擷取功能可擷取和儲存無線存取點(WAP)接收和傳輸封包。捕獲的資料包隨後可由網路協定分析器進行分析，以進行故障排除或效能最佳化。封包擷取有兩種方法：

- 在此裝置上儲存檔案 — 捕獲的資料包儲存在WAP上的檔案中。WAP還可以將檔案傳送到簡單式檔案傳輸協定(TFTP)伺服器。檔案管理資料包捕獲的格式為pcap格式，可以使用Wireshark和OmniPeek等工具檢查。
- 流到遠端主機 — 捕獲的資料包被即時重定向到運行Wireshark工具的外部電腦。

本文旨在解釋和指導您在WAP上配置資料包捕獲，並在本地或遠端接收這些資料包捕獲。

適用裝置

- WAP125
- WAP581

軟體版本

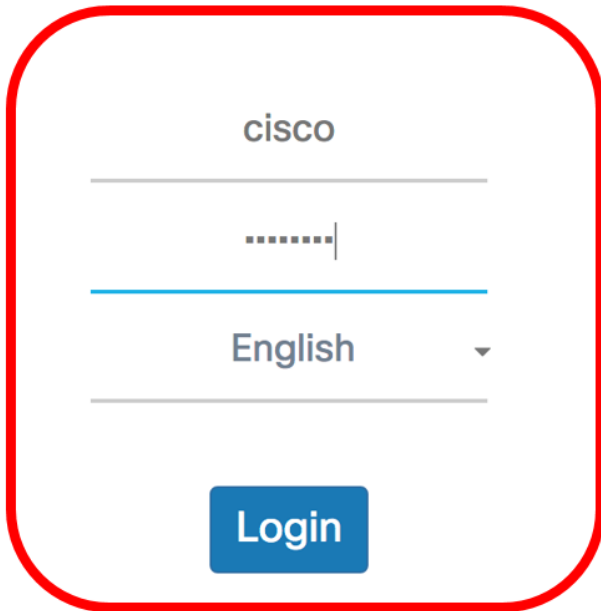
- 1.0.0.4 - WAP581
- 1.0.0.5 - WAP125

配置資料包捕獲設定

步驟1.登入到WAP的基於Web的實用程式。預設使用者名稱和密碼為cisco/cisco。



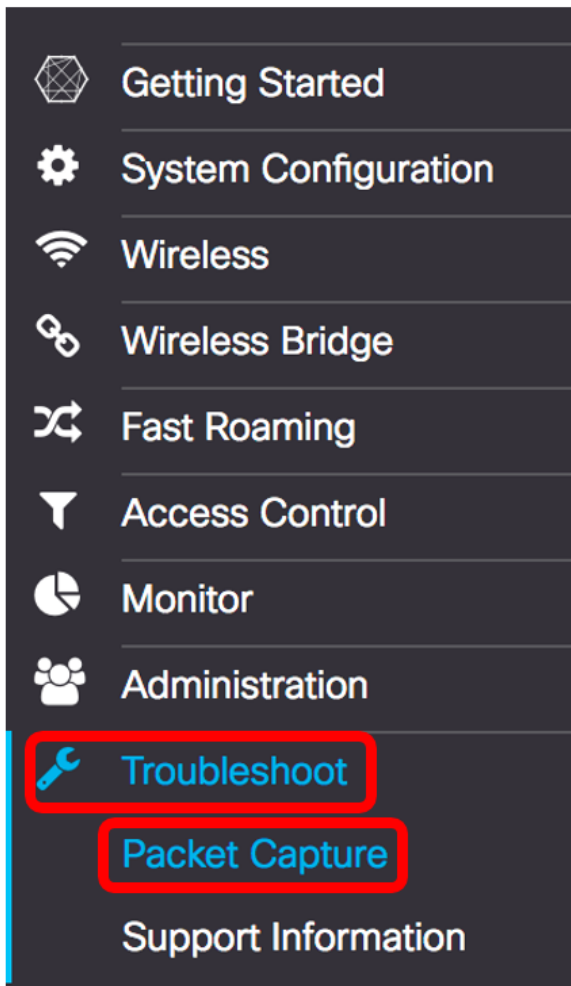
Wireless Access Point

A login form for a Cisco Wireless Access Point. It features a red rounded rectangular border. Inside, there is a text input field containing "cisco", a password input field with a masked password ".....|", a language selection dropdown menu currently set to "English", and a blue "Login" button at the bottom.

附註：如果您已更改密碼或建立新帳戶，請輸入您的新憑據。

步驟2.選擇Troubleshoot > Packet Capture。

附註：可用選項可能會因裝置的具體型號而異。本示例使用WAP125。



步驟3.選擇以下資料包捕獲方法單選按鈕之一：

- 在此裝置上儲存檔案 — 將捕獲的資料包儲存為WAP上的檔案。配置要在本地儲存的介面、持續時間和最大檔案大小。
- 流到遠端主機 — 將捕獲的資料包即時重定向到運行網路協定分析器工具的外部電腦。如果選擇此選項，請跳至步驟7。

附註：在本示例中，選擇在此裝置上儲存檔案。

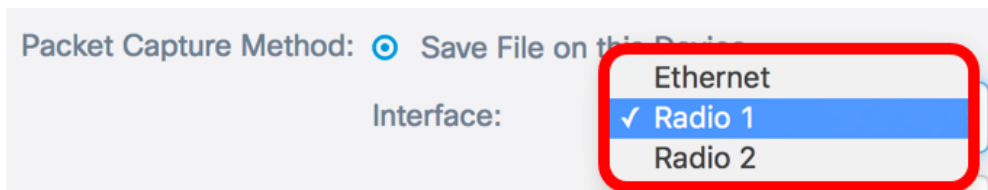
A configuration screen for Packet Capture Method. It shows two radio buttons: 'Save File on this Device' (selected) and 'Stream to a Remote Host'. Under 'Save File on this Device', there are three input fields: 'Interface' (Radio 1), 'Duration' (60 Sec.), and 'Max File Size' (1024 KB). Under 'Stream to a Remote Host', there is one input field: 'Remote Capture Port' (2002).

步驟4.從Interface下拉選單中，從Capture Interface下拉選單中選擇要為其捕獲資料包的介面。選項包括：

- 乙太網 — 乙太網埠上的802.3流量。
- Radio 1 — 無線介面1上的802.11流量。

- Radio 2 — 無線介面2上的802.11流量。

附註：在本示例中，選擇無線電1。

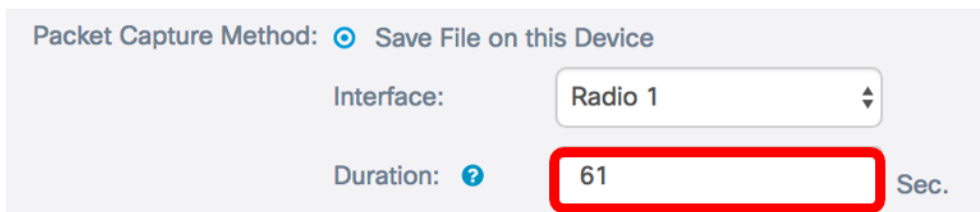


Packet Capture Method: Save File on this Device

Interface: Ethernet
✓ Radio 1
Radio 2

步驟5.在 *Duration* 欄位中輸入捕獲持續時間，範圍為10到3600秒。預設值為60秒。

附註：在此示例中，使用61。

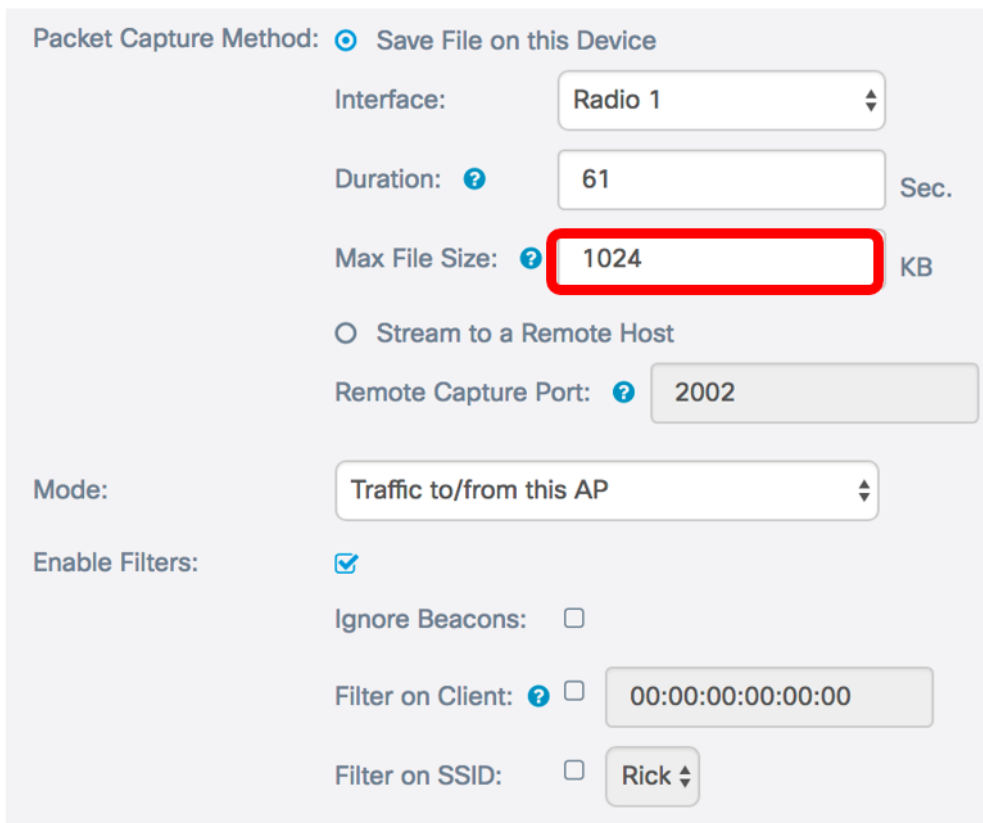


Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: Sec.

步驟6.在 *Max File Size* 欄位中，輸入最大擷取檔案大小，範圍從64到4096 KB，然後跳到步驟8。預設值為1024 KB。



Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: Sec.

Max File Size: KB

Stream to a Remote Host

Remote Capture Port:

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client:

Filter on SSID: Rick

附註：在此範例中使用預設值。

步驟7.如果選擇遠端資料包捕獲方法，請在 *遠端捕獲埠* 欄位中輸入從1到65530的埠號。預設值為2002。

Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: 61 Sec.

Max File Size: 1024 KB

Stream to a Remote Host

Remote Capture Port: 2002

附註：在本範例中，使用預設連線埠。

步驟8.從Mode下拉選單中，選擇將捕獲的資料包。選項包括：

- 所有無線流量 — 擷取所有無線封包，包括在其他網路上傳送的無線封包。
- 此AP的流量捕獲在WAP和客戶端之間傳送的資料包。在此範例中，選擇了此選項。

Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: 61 Sec.

Max File Size: 1024 KB

Stream to a Remote Host

Remote Capture Port: 2002

Mode: Traffic to/from this AP

步驟9.選中Enable Filters覈取方塊以允許對封包擷取使用特定過濾器。

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

步驟10。（可選）選中Ignore Beacons 覈取方塊以禁用捕獲無線電檢測到或傳輸的802.11信標。信標幀被週期性地傳送以通告無線區域網(WLAN)的存在。

附註：在此示例中，啟用忽略信標。

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

步驟11。(可選)選中**Filter on Client**釁取方塊以指定無線客戶端的MAC地址。

附註：在本例中，Filter on Client未選中。

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

步驟12。(可選)在**Filter on Client**欄位中輸入客戶端的MAC地址。僅當在無線電介面上執行資料包捕獲時，此選項才處於活動狀態。

附註：在此範例中，使用者端上的篩選功能已停用。

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

步驟13.選中**Filter on SSID**釁取方塊以捕獲特定SSID上的資料包。

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

步驟14.從SSID下拉選單中選擇一個SSID以捕獲資料包。

附註：下拉選單中顯示的SSID取決於選擇的介面和已配置的SSID數量。在本示例中，選擇了Rick。

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

步驟15.按一下**Save**按鈕以儲存已設定的設定。

Packet Capture

Save

Packet Capture Method: Save File on this Device

Interface: Radio 1

Duration: 61 Sec.

Max File Size: 1024 KB

Stream to a Remote Host

Remote Capture Port: 2002

Mode: Traffic to/from this AP

Enable Filters:

Ignore Beacons:

Filter on Client: 00:00:00:00:00:00

Filter on SSID: Rick

您現在應該已經成功配置資料包捕獲設定。

封包擷取

步驟16. 「資料包捕獲狀態」區域包含以下資訊。按一下**刷新**以檢視當前狀態。





Packet Capture Status

Current Capture Status: Stopped due to administrative action

Packet Capture Time: 00:00:17

Packet Capture File Size: 1024 KB

Refresh

- Current Capture Status — 顯示當前資料包捕獲狀態。在本例中，— 由於管理操作而停止 — 是當前狀態。
- Packet Capture Time — 顯示捕獲資料包的持續時間。在本示例中，記錄了00:00:17秒。
- Packet Capture File Size — 顯示資料包捕獲檔案的大小。在本例中，1024kb是捕獲大小。

步驟17. 按一下**Start Capture**按鈕開始資料包捕獲過程。





Packet Capture Status

Current Capture Status: Not started


Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

Refresh

步驟18.將彈出一個視窗，通知您現在將開始資料包捕獲。按一下OK繼續。

 Do you want to start file capture now?

OK cancel

步驟19.按一下Stop Capture按鈕停止資料包捕獲過程。





Packet Capture Status

Current Capture Status: Not started

Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

Refresh

步驟20.將彈出一個視窗，通知您確認結束資料包捕獲。按一下OK繼續。

Alert

×



Stop packet capture.

OK

現在，您應該已經成功捕獲了接入點上的資料包。

封包擷取檔案下載

下載到此裝置

步驟1. 按一下Download to this Device按鈕。

Packet Capture Status

Current Capture Status: Not started

Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

Refresh

▶ || ⬇️ ⬇️

步驟2. 將彈出視窗開始下載。按一下「OK」。

Confirm

×



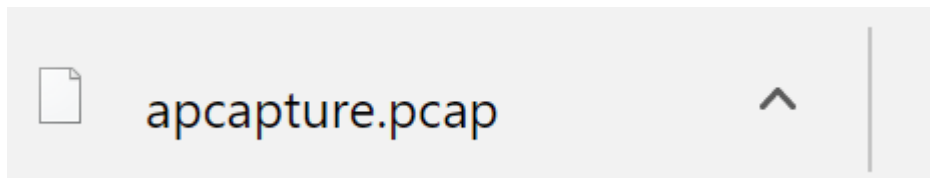
The file is downloading now.

OK

cancel

下載完成後，下載的檔案將顯示在瀏覽器下載歷史記錄中。檔案是以HTTP/HTTPS下載，且檔案格式為.pcap。

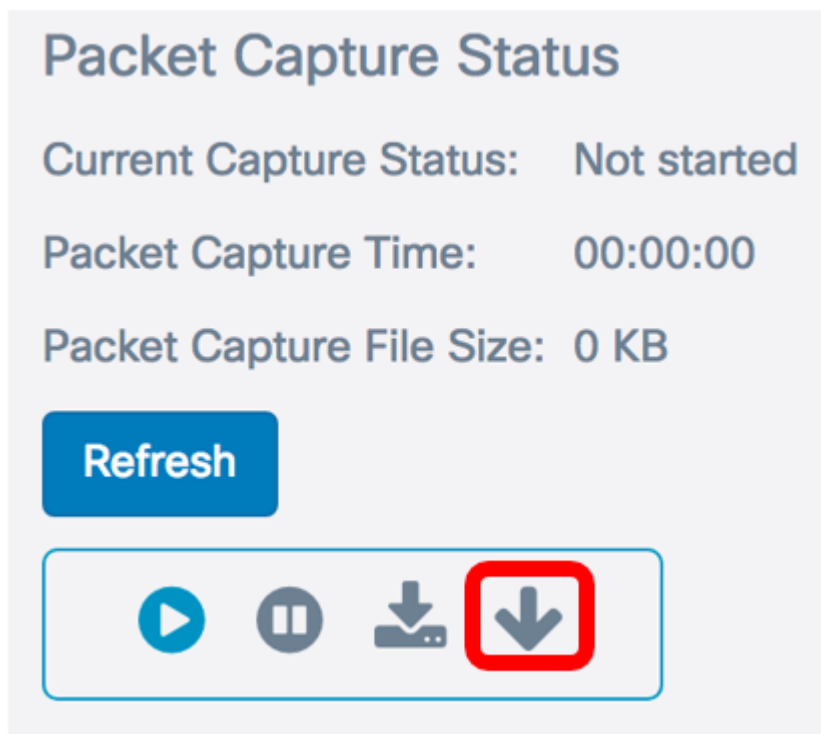
附註：在本示例中，apcapture.pcap是下載的檔案。



您已成功將WAP的資料包捕獲檔案下載到您的電腦。

下載到TFTP伺服器

步驟1。（可選）如果必須通過TFTP伺服器下載捕獲的檔案，請按一下Download to TFTP Server 按鈕。



按一下後，將出現一個視窗，其中包含「伺服器IPv4地址」和「目標檔名」欄位。

Download File Using TFTP

Server IPv4 Address ?

Destination File Name ?


Download


cancel

步驟2.在Server IPv4 Address欄位中輸入TFTP伺服器的IPv4地址。然後，在第6步的Remote Capture Port欄位中輸入的埠號會連線到TFTP伺服器地址。

附註：本示例使用128.12.8.128。

Download File Using TFTP


Server IPv4 Address 


Destination File Name 

步驟3.在「*Destination File Name*」欄位中，以pcap格式輸入檔案名稱。

附註：在本示例中，使用了apcapture.pcap。


Download File Using TFTP


Server IPv4 Address 

Destination File Name 

步驟4.按一下Download。

Download File Using TFTP

Server IPv4 Address 

Destination File Name 

Destination File Name 欄位下方會顯示進度欄。

Download File Using TFTP

Server IPv4 Address  128.12.8.128

Destination File Name  apcapture.pcap



Download

cancel

您現在應該已經通過TFTP伺服器下載了資料包捕獲檔案。