在WAP121和WAP321接入点上配置数据包捕获

目标

数据包捕获是网络设备的一项功能,它使您能够捕获和存储设备发送和接收的数据包。网络协 议分析器可以分析捕获的数据包,以排除故障或优化性能。捕获的数据包文件可以通过 HTTP/HTTPS或TFTP下载。可以共享数据包,然后进一步分析以了解网络中的数据包流。

本文档旨在说明如何在WAP121和WAP321接入点(AP)上配置数据包捕获和下载数据包捕获文件。

适用设备

·WAP121 · WAP321

软件版本

·1.0.3.4(WAP121和WAP321)

数据包捕获配置

步骤1.登录Web配置实用程序,然后选择Administration>Packet Capture**。**"数*据包捕*获"页打 开:

Packet Capture		
Packet Capture Configuration		
Capture Beacons:	C Enable	
Promiscuous Capture:	Enable	
Radio Client Filter:	V Enable	
Client Filter MAC Address:	4B:DC:88:06:6C:4C	(xxcxxcxxcxxcxxx)
Packet Capture Method:	Local File	
	Remote	
Capture Interface:	•	
Capture Duration:	60	Second (Range: 10-3600, Default: 60)
Maximum Capture File Size:	1024	KB (Range: 64-4096, Default: 1024)
Remote Capture Port:	2002	(Range:1025-65530, Default: 2002)
Save Start Capture Stop Capture		

步骤2.选中Capture Beacons**字**段的Enable复选框。定期传输信标帧以通告存在无线LAN网络。

步骤3.选中以下字段之一旁的以下复选框之一以选择特定捕获选项:

·混杂捕获 — 这使无线网络接口卡(NIC)可捕获所有数据包,无论它是否用于此设备。

·Radio Client Filter — 这使无线网卡仅从WLAN客户端捕获数据包。

注意:不能同时启用混合捕获和无线电客户端过滤器。

注意:如果已选择混杂捕获模式,请跳过步骤4。

步骤4.如果启用了Radio Client Filter,请在Client Filter MAC Address字段中输入客户端过*滤* 器的MAC地址。

步骤5.单击Packet Capture Method单选按钮之一。

·本地文件 — 将捕获的数据包作为文件存储在AP设备上。文件采用pcap格式,AP可以将文 件传输到TFTP服务器。如果选择此选项,请跳过步骤7。

·远程 — 将捕获的数据包实时重定向到运行网络协议分析器工具的外部计算机。如果选择此 选项,请跳过步骤6。

步骤6.如果选择Local File,请配置这些字段。

Client Filter MAC Address:	00:00:00:00:00:00	(XXXXXXXXXXXXXXX)	
Packet Capture Method:	 Local File Remote 		
Capture Interface:	radio1 💌		
Capture Duration:	88	Second (Range: 10-3600, Default: 60)	
Maximum Capture File Size:	2020	KB (Range: 64-4096, Default: 1024)	
Remote Capture Port:	2002	, (Range:1025-65530, Default: 2002)	
Save Start Capture Stop Capture			

·捕获接口 — 在捕获接口(Capture Interface)下拉列表中,选择要捕获数据包的接口。下拉列 表包含接口brtrunk、radio1、etho和vap0。

·捕获持续时间 — 输入捕获持续时间(以秒为单位)。这范围为10到3600秒。

·最大捕获文件大小 — 输入最大捕获文件大小(KB)范围,范围从64 KB到4096 KB。

步骤7.如果选择远程数据包捕获方法,请在Remote Capture Port字段中输入从1到65530的端 口号范围。默认值为 2002。

Packet Capture	
Packet Capture Configuration	
Capture Beacons:	👿 Enable
Promiscuous Capture:	Enable
Radio Client Filter:	Enable
Client Filter MAC Address:	00:00:00:00:00:00
Packet Capture Method:	Local FileRemote
Capture Interface:	radio1 💌
Capture Duration:	60
Maximum Capture File Size:	1024
Remote Capture Port:	2002
Save Start Capture Stop Capture	

步骤8.单击"**保存**"以保存设置。

步骤9.单击Start Capture(开始捕获)开始数据包捕获过程。

步骤10.系统将显示警报消息。单击OK继续数据包捕获过程。

Confirm					\times
	Make sure remote monitor capture?	ing applic	ation is ready.	Start remote packet	
	O	<	Cancel		

步骤11.单击**停止捕**获以停止数据包捕获进程。数据包捕获状态区域显示捕获正在进行。

Save Start Capture Stop Capture			
Packet Capture Status			
Current Capture Status:	File capture in progress		
Packet Capture Time:	0		
Packet Capture File Size:	0 KB		
Refresh			

步骤12.系统将显示警报消息。单击OK以停止数据包捕获过程。



数据包捕获状态

步骤1. Packet Capture Status区域包含以下信息。单击Refresh获取最近的状态。

Save Start C	apture Stop Capture		
Packet Capture Status			
Current Capture Status:	File capture in progress		
Packet Capture Time:	0		
Packet Capture File Size:	0 KB		
Refresh			

·当前捕获状态 — 显示当前数据包捕获状态。

·数据包捕获时间 — 显示捕获数据包的时间。

·数据包捕获文件大小 — 显示捕获的数据包文件的大小。

数据包捕获文件下载

步骤1.(可选)如果捕获的文件必须通过TFTP服务器下载,请选中**Use TFTP to download the capture file复选框。**TFTP Server Filename字段和TFTP Server IPv4 Address字段激活。

Packet Capture File Download			
File download using HTTP/HTTPS may be done by simply clicking the Download button. To use TFTP download,			
Use TFTP to download the capture file			
TFTP Server Filename:	apcapture.pcap	(Range: 1 - 256 Characters)	
TFTP Server IPv4 Address:	192.168.78.0	(x000.3000.3000)	
Download			

节省时间:如果不选中步骤1中的复选框,请跳至步骤4。

步骤2.在TFTP Server Filename字段中输入pcap格式的文件名。

步骤3.在TFTP Server IPv4 Address字段中输入TFTP服务器的IPv4地址。

步骤4.单击**Download**。如果未选择TFTP,则文件将使用HTTP/HTTPS下载,此时会出现一个 窗口,通知您下载正在进行。Click OK.

Capture Duration:	60		Second (Range: 10-3600, Default: 60)
Maximum Capture File Siz	Confirm		
Remote Capture Port:	The file is downloading now.		
Save Start			OK Cancel
Packet Capture Status			
Current Capture Status:	Stopped due to administrative action		
Packet Capture Time:	00:00:13		
Packet Capture File Size:	213 KB		
Refresh			
Packet Capture File Dov	vnload		
File download using HTTP/	HTTPS ma	y be done by simp	ly clicking the Download button. To use TFTP download, check the b
Use TFTP to download the capture file			
TFTP Server Filename:	apcapti	ле.рсар	(Range: 1 - 256 Characters)
TFTP Server IPv4 Address	: 0.0.0.0		(x00C300C300C)
Download			

注意:您可以使用开源的Wireshark软件解释和理解从数据包捕获中获取的信息。

在Wireshark中查看捕获的数据包

步骤1.启动Wireshark软件。

WIRESHARK The World's Most Popular Network Version 1.8.2 (SVN Rev 44520 from /trun	The World's Most Popular Network Protocol Analyzer Version 1.8.2 (SVN Rev 44520 from /trunk-1.8)		
Capture	Files		
No interface can be used for capturing in this system with the current configuration. See Capture Help below for details.	Open Open a previously captured file Open Recent: C:\Users\caesar\Downloads\apcapture.pcap [not found] Image: Sample Captures A rich assortment of example capture files on the wiki		

步骤2.单击"文件"部分中的"打开",浏览并从PC中选择捕获文件。

步骤3.在PC上查找文件。

步骤4.打开以查看捕获的文件。