在WAP351上配置802.1X設定

目標

IEEE 802.1X身份驗證允許WAP裝置訪問安全的有線網路。您可以將WAP裝置配置為有線網路上的802.1X請求方(客戶端)。WAP351還可以配置為身份驗證器。可以配置加密的使用 者名稱和密碼以允許WAP裝置使用802.1X進行身份驗證。

在使用基於IEEE 802.1X埠的網路訪問控制的網路上,請求方無法訪問該網路,直到802.1X驗 證方授予訪問許可權。如果您的網路使用802.1X,您必須在WAP裝置上設定802.1X驗證資訊 ,以便它能將其提供給驗證器。

本文檔的目標是向您展示如何在WAP351上配置802.1X Supplicant客戶端設定。

適用裝置

·WAP351

軟體版本

·v1.0.1.3

配置802.1X請求方設定

步驟1.登入到Web配置實用程式並選擇System Security > 802.1X。802.1X頁面隨即開啟。

302.1X					
Port Table					
	Port No.	Enable	Role		
	1		Supplicant 💌	Show Details	
	2		Supplicant -	Show Details	
	3		Supplicant -	Show Details	
	4		Supplicant -	Show Details	
	5		Supplicant -	Show Details	
Edit					
Sav	e				

步驟2. *連線埠表*顯示五個可設定為802.1X驗證的LAN介面。勾選與您要編輯的連線埠對應的 覈取方塊。

802.1X					
Port	Table				
	Port No.	Enable	Role		
			Supplicant 🔹	Show Details	
	2		Supplicant -	Show Details	
	3		Supplicant 💌	Show Details	
	4		Supplicant -	Show Details	
	5		Supplicant -	Show Details	
Edit					
Save					

步驟3.按一下Edit按鈕。選中的埠現在可用於編輯。

802.1X					
Port	Table				
	Port No.	Enable	Role		
V			Supplicant 🔹	Show Details	
	2		Supplicant 💌	Show Details	
	3		Supplicant 💌	Show Details	
	4		Supplicant 💌	Show Details	
	5		Supplicant 💌	Show Details	
Edit					
Sav	e				

步驟4.在Enable欄位中,勾選您要在其上啟用802.1X設定的連線埠的覈取方塊。

802.1X						
Por	t Table					
	Port No.	Enable	Role			
V			Supplicant	•	Show Details	
	2		Supplicant	-	Show Details	
	3		Supplicant	•	Show Details	
	4		Supplicant	•	Show Details	
	5		Supplicant	•	Show Details	
Edit						
Sa	ave					

步驟5.在*Role*下拉選單中,選擇將相應的埠配置為Supplicant客戶端還是Authenticator。如果 選擇了Supplicant客戶端,請轉到<u>Supplicant Settings Configuration</u>部分。如果選擇驗證器 ,請轉到<u>驗證器設定配置</u>部分。驗證器位於想要存取網路的使用者端(要求者)和RADIUS伺 服器本身之間。它負責處理兩者之間的所有通訊。請求方向身份驗證器提供憑證以訪問網路。 WAP351上的典型設定將使WAN埠成為請求方(因此WAP可以訪問網路),並使LAN埠成為 驗證方(因此WAP可以授權其下面的裝置)。

8	802.1X					
	Port	Table				-
		Port No.	Enable	Role		
	V		V	Supplicant 🔻	Show Details	
		2		Supplicant Authenticator	Show Details	
		3		Supplicant 💌	Show Details	
		4		Supplicant 💌	Show Details	
		5		Supplicant 💌	Show Details	
	Edit					
	Sav	e				

請求方設定配置

步驟1.按一下Show Details以顯示請求方設定資訊。

Port	Table		
	Port No.	Enable	Role
V		✓	Supplicant Hidden Details
	Port No.		Kole Supplicant Image: 1 - 64 Characters) Username: Image: 1 - 64 Characters) Password: Image: 1 - 64 Characters) Password: Image: 1 - 64 Characters) Certificate File Status Refresh Certificate File Present: No Certificate Expiration Date: Not Present Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information. Certificate File Upload Transfer Method: Image: HTTP Image: TFTP
	2		Filename Browse No file selected.

附註:在模式欄位中進行選擇後,此資訊可能會自動開啟。

步驟2.在*EAP Method*下拉選單中,選擇用於加密使用者名稱和密碼的演算法。EAP代表可擴展身份驗證協定,並用作加密演算法的基礎。

EAP Method: MD5						
Username: PEAP TLS	(Range: 1 - 64 Characters)					
Password:	(Range: 1 - 64 Characters)					
Certificate File Status Refresh						
Certificate File Present: No						
Certificate Expiration Date: Not Present						
Browse to the location where your certificate file is stored and cli To upload from a TFTP server, click the TFTP radio button and e	Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TETP server, click the TETP radio button and enter the TETP server information					
Certificate File Upload						
Transfer Method: HTTP TFTP 						
Filename Browse No file selected.						
Upload						

可用選項包括:

·MD5 - MD5消息摘要演算法利用雜湊函式來提供基本的安全性。不建議使用此演算法,因為 其他兩個具有更高的安全性。

·PEAP - PEAP代表受保護的可擴展身份驗證協定。它封裝了EAP,通過使用TLS隧道傳輸資料,可提供比MD5更高的安全性。

·TLS — TLS代表傳輸層安全性,是提供高安全性的開放標準。

步驟3.在Username欄位中,輸入WAP裝置在回應802.1X驗證器要求時將使用的使用者名稱。 使用者名稱長度必須為1到64個字元,並且可以包含字母數字字元和特殊字元。

EAP Method:	MD5	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)
Certificate File Statu	Refresh	
Certificate File Present	: No	
Certificate Expiration D	ate: Not Present	
Browse to the location To upload from a TFTP	where your certificate file is stored and cli server, click the TFTP radio button and e	ck the "Upload" button. nter the TFTP server information.
Certificate File Uploa	d	
Transfer Method:	HTTP TFTP	
Filename	owse No file selected.	
Upload		

步驟4.在*密碼*欄位中,輸入WAP裝置在回應802.1X驗證器要求時將使用的密碼。使用者名稱 長度必須為1到64個字元,並且可以包含字母數字字元和特殊字元。

EAP Method:	MD5	
Username:	username1	(Range: 1 - 64 Characters)
Password:		(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	where your certificate file is stored and of server, click the TFTP radio button and	click the "Upload" button. enter the TFTP server information.
Certificate File Upload		
Transfer Method: <a>H H	TTP FTP	
Filename Bro	wse No file selected.	
Upload		

步驟5. Certificate File Status區域顯示WAP裝置上是否存在HTTP SSL證書檔案。如果憑證存 在, Certificate File Present欄位會顯示「Yes」;預設值為「No」。如果存在證書,則會顯 示*證書到期日*;否則,預設值為「Not present」。要顯示最新資訊,請按一下**Refresh**按鈕以獲 得最新的證書資訊。

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Stat	tus Refresh	
Certificate File Prese	ent: No	
Certificate Expiration	Date: Not Present	
Browse to the locatio To upload from a TF	on where your certificate file is stored and cl TP server, click the TFTP radio button and e	ick the "Upload" button. enter the TFTP server information.
Certificate File Upl	oad	
Transfer Method: <a>©	HTTP TFTP	
Filename	Browse No file selected.	
Upload		

步驟6。如果您不想上傳HTTP SSL憑證檔案,請跳至<u>步驟12</u>。否則,在**Transfer Method**欄位 中選擇「HTTP」或「TFTP」單選按鈕以選擇要用於上傳憑證的通訊協定。

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	here your certificate file is stored and cli server, click the TFTP radio button and e	ck the "Upload" button. hter the TFTP server information.
Certificate File Upload		
Transfer Method: 💿 H 🔘 TI	TTP FTP	
Filename	wse No file selected.	
Upload		

步驟7.如果選擇**TFTP**,請繼續步驟8。如果選擇**HTTP**,請按一下**Browse...**按鈕在PC上查詢證 書檔案。跳至<u>步驟10</u>。

EAP Method:	MD5	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	here your certificate file is stored and cli server, click the TFTP radio button and e	ck the "Upload" button. nter the TFTP server information.
Certificate File Upload		
Transfer Method: H T T	TTP FTP	
Filename Bro	wse No file selected.	
Upload		

步驟8.如果您在*Transfer Method*欄位中選擇了**TFTP**,請在*Filename*欄位中輸入憑證的名稱。

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status Certificate File Present:	Refresh	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	here your certificate file is stored and cli server, click the TFTP radio button and e	ck the "Upload" button. nter the TFTP server information.
Certificate File Upload		
Transfer Method:	HTTPTFTP	
Filename	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Addre	ss:	(xxx.xxx.xxx)
Upload		

附註:檔案必須以.pem結尾。

步驟9.在「TFTP Server IPv4 Address」欄位中輸入TFTP伺服器的IP地址。

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Status	Refresh	
Certificate File Present:	No	
Certificate Expiration Da	te: Not Present	
Browse to the location w To upload from a TFTP s	here your certificate file is stored and clic server, click the TFTP radio button and er	ck the "Upload" button. hter the TFTP server information.
Certificate File Upload		
Transfer Method:	HTTPTFTP	
Filename	certificate.pem	(Range: 1 - 256 Characters)
TFTP Server IPv4 Addre	ss: 192.0.2.100	
Upload		

<u>步驟10</u>.按一下Upload。

EAP Method:	MD5 💌	
Username:	username1	(Range: 1 - 64 Characters)
Password:	•••••	(Range: 1 - 64 Characters)
Certificate File Statu	Is Refresh	
Certificate File Preser	t: No	
Certificate Expiration I	Date: Not Present	
Browse to the location To upload from a TFT	where your certificate file is stored an P server, click the TFTP radio button a	nd click the "Upload" button. nd enter the TFTP server information.
Certificate File Uplo	ad	
Transfer Method: <a>O	HTTP TFTP	
Filename	rowse certificate.pem	
Upload		

步驟11.出現確認視窗。按一下「OK」開始上傳。

Dev	ce is uploading the certificate file now.
	OK Cancel
Certificate File	Present: No
Certificate Ex	piration Date: Not Present
Browse to the To upload from	location where your certificate file is stored and click the "Upload" button. n a TFTP server, click the TFTP radio button and enter the TFTP server informati
Browse to the To upload fror Certificate F	location where your certificate file is stored and click the "Upload" button. n a TFTP server, click the TFTP radio button and enter the TFTP server informati Ie Upload
Browse to the To upload fror Certificate F Transfer Meth	e location where your certificate file is stored and click the "Upload" button. n a TFTP server, click the TFTP radio button and enter the TFTP server informati i le Upload od: O HTTP TFTP
Browse to the To upload fror Certificate F Transfer Meth Filename	e location where your certificate file is stored and click the "Upload" button. In a TFTP server, click the TFTP radio button and enter the TFTP server informati Ile Upload od: O HTTP TFTP Browse certificate.pem

步驟12.對要配置為802.1X請求方的每個埠重複此部分。然後按一下Save。

Port Table						
	Port No.	Enable	Role			
v		V	Supplicant	•	Show Details	
	2		Supplicant	-	Show Details	
	3		Supplicant	-	Show Details	
	4		Supplicant	-	Show Details	
	5		Supplicant	-	Show Details	
Edit						

<u>身份驗證器設定配置</u>

步驟1.按一下Show Details以顯示驗證器設定資訊。

Port	Table						
	Port No.	Enable	Role				
V		✓	Authenti	cator 💌 🖡	Hidden Details		
	Use global RADIUS server settings Server IP Address Type: IPv4 IPv6						
			No.	Server IP A	ddress x.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
			1	0.0.0.0			1812
			2				1812
			3				1812
			4				1812
		Enable RADIUS Accounting Active Server: Server IP Address-1 • Periodic Reauthentication: Enable Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)					
	2		Supplica	ant 🔻 S	Show Details		

附註:在模式欄位中進行選擇後,此資訊可能會自動開啟。

步驟2.如果您希望連線埠在驗證期間使用全域RADIUS設定,請勾選*使用全域RADIUS伺服器 設定*覈取方塊。如果您希望連線埠使用不同的RADIUS伺服器(或伺服器),請取消選中此覈 取方塊;否則,請跳至<u>步驟8</u>。

Us Server	se global RADIUS ser r IP Address Type: 🤅	ver settings IPv4 IPv6	•			
No.	Server IP Address (XXXX.XXXX.XXXX)		Key (Range: 1 - 64	Characters)	Auth (Ra	entication Port nge: 0 - 65535, Default: 1812)
1	0.0.0.0				1	812
2					1	812
3					1	812
4					1	812
E	Enable RADIUS Accou	unting				
Active	Server:	Server IP	Address-1 💌			
Period	lic Reauthentication:	Enabl	le			
Reaut	hentication Period:	3600		sec. (Range: 3	300 - 4	294967295, Default: 3600)

附註:有關詳細資訊,請參閱在WAP131和WAP351上配置全域性RADIUS伺服器設定一文。

步驟3.在「Server IP Address Type」欄位中,選擇RADIUS伺服器使用的IP版本的單選按鈕

。可用的選項有IPv4和IPv6。

Us Server	Use global RADIUS server settings Server IP Address Type: IPv6 IPv6						
No.	Server IP Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		Key (Range: 1 - 64	Characters)	Au (R	thentication Port lange: 0 - 65535, Default: 1812)	
1	0.0.0.0					1812	
2						1812	
3						1812	
4						1812	
E Activo	Enable RADIUS Accour		Addross 1 💌				
Active	Server.	Serverin	Address-1				
Period	lic Reauthentication:	Enabl	le				
Reaut	hentication Period:	3600		sec. (Range: 3	- 00	4294967295, Default: 3600)	

附註:您可以在地址型別之間切換以配置IPv4和IPv6 RADIUS地址設定,但WAP裝置僅聯絡 具有您在此欄位中選擇的地址型別的RADIUS伺服器。不能讓多個伺服器在一個配置中使用不 同的地址型別。

步驟4.在*Server IP Address 1*或*Server IPv6 Address 1*欄位中,根據您在步驟3中選擇的地址 型別,輸入RADIUS伺服器的IPv4或IPv6地址。

🔲 Us	Use global RADIUS server settings					
Server	r IP Address Type: 🤅	IPv4 IPv6				
No.	Server IP Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Key (Range: 1 - 6-	4 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)		
1	192.0.2.1			1812		
2				1812		
3				1812		
4				1812		
E	Enable RADIUS Acco	unting				
Active	Server:	Server IP Address-1				
Period	lic Reauthentication:	Enable				
Reaut	hentication Period:	3600	sec. (Range: 30	0 - 4294967295, Default: 3600)		

附註:在此欄位中輸入的地址將指定埠的主RADIUS伺服器。在後續欄位(伺服器IP地址2至4

)中輸入的地址將指定在主伺服器身份驗證失敗時按順序嘗試的備份RADIUS伺服器。

步驟5.在*Key*欄位中,輸入與WAP裝置用來向RADIUS伺服器驗證的主要RADIUS伺服器對應 的共用金鑰。可以使用1到64個標準字母數字和特殊字元。在*Key 2*至4欄位中針對連線埠設定 的每個後續的RADIUS伺服器重複此步驟。

🔲 Us	Use global RADIUS server settings					
Server	r IP Address Type: 🤅	IPv4 IPv6				
No.	Server IP Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1		1812			
2			1812			
3			1812			
4			1812			
E	Enable RADIUS Accou	inting				
Active	Server:	Server IP Address-1				
Period	lic Reauthentication:	Enable				
Reaut	hentication Period:	3600 sec. (Range:	300 - 4294967295, Default: 3600)			

附註:這些金鑰區分大小寫,並且必須與RADIUS伺服器上配置的金鑰相匹配。

步驟6.在Authentication Port欄位中,輸入WAP將用來連線到RADIUS伺服器的連線埠。在 Authentication Port 2至4 欄位中設定的每個備份RADIUS伺服器重複此步驟。預設值為 1812。

C Us Server	Use global RADIUS server settings Server IP Address Type: IPv4 IPv6					
No.	Server IP Address (XXX.XXX.XXX.XXX)		Key (Range: 1 - 64	Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)	
1	192.0.2.1		•••••	•	1812	
2					1812	
3					1812	
4					1812	
E E	Enable RADIUS Accou					
Active	Server.	Server	Address-1			
Period	lic Reauthentication:	Enab	le			
Reaut	hentication Period:	3600		sec. (Range: 3	300 - 4294967295, Default: 3600)	

步驟7.選中**啟用RADIUS記帳**覈取方塊以啟用跟蹤和測量使用者已使用的資源(系統時間、傳輸的資料量等)。選中此覈取方塊將為主伺服器和備份伺服器啟用RADIUS記帳。

🔲 U:	Use global RADIUS server settings					
Serve	r IP Address Type: 🧕	IPv4 IPv6				
No.	Server IP Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Key (Range: 1 - 64 Chara	cters) Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
	Enable RADIUS Accou	unting				
Active	Server:	Server IP Address-1				
Period	dic Reauthentication:	Enable				
Reaut	Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)					

步驟8.在「Active Server」下拉選單中,選擇其中一個已配置的RADIUS伺服器以設定為活動 伺服器。此設定允許WAP立即嘗試聯絡活動伺服器,而不是嘗試按順序聯絡每台伺服器並選 擇第一個可用伺服器。

 Use global RADIUS server settings Server IP Address Type: IPv4 IPv6 						
No.	Server IP Address (XXXX.XXXX.XXXX)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
Enable RADIUS Accounting						
Active Server: Server IP Address-1						
Periodic Reauthentication: Server IP Address-1 Server IP Address-2 Server IP Address-3 Server IP Address-4 Server IP Address-4 Server IP Address-4 Server IP Address-4						

步驟9.在*Periodic Reauthentication*欄位中,選中**Enable**覈取方塊以啟用EAP重新身份驗證。 如果您不想啟用EAP重新身份驗證,請跳至<u>步驟11</u>。

Use global RADIUS server settings						
Server IP Address Type: IPv4 IPv6 						
No.	Server IP Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Key (Range: 1 - 64 Characters	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
Enable RADIUS Accounting						
Active Server IP Address-1						
Periodic Reauthentication: Enable						
Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)						

步驟10.如果在*Periodic Reauthentication*欄位中選中**Enable**覈取方塊,請在*Reauthentication Period*欄位中輸入EAP重新身份驗證時間段(以秒為單位)。預設值為3600。有效範圍為300 - 4294967295秒。

Use global RADIUS server settings Server IP Address Type: IPv4 IPv6						
No.	Server IP Address (XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)			
1	192.0.2.1	•••••	1812			
2	192.0.2.2	•••••	2500			
3			1812			
4			1812			
Image: Server IP Address-1						
Periodic Reauthentication: 🗹 Enable						
Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)						

<u>步驟11</u>.對要配置為802.1X驗證器的每個埠重複此部分。然後按一下**Save**。

802.1X								
Port	Port Table							
	Port No.	Enable	Role					
		V	Authenticator	•	Show Details			
	2		Supplicant	•	Show Details			
	3		Supplicant	•	Show Details			
	4		Supplicant	•	Show Details			
	5		Supplicant	•	Show Details			
E	Edit							
Sav	e							