WEP auf einem autonomen Access Point -Konfigurationsbeispiel

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Authentifizierungsmethoden Konfigurieren GUI-Konfiguration CLI-Konfiguration Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird die Verwendung und Konfiguration von Wired Equivalent Privacy (WEP) auf einem unabhängigen Cisco Access Point (AP) beschrieben.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie eine administrative Verbindung zu den WLAN-Geräten herstellen können und dass die Geräte in einer unverschlüsselten Umgebung normal funktionieren. Um ein standardmäßiges 40-Bit-WEP zu konfigurieren, müssen zwei oder mehr Funkeinheiten miteinander kommunizieren.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Access Point der Serie 1140, auf dem Cisco IOS[®] Release 15.2JB ausgeführt wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

WEP ist der in den 802.11-Standard (Wi-Fi) integrierte Verschlüsselungsalgorithmus. WEP verwendet die <u>Stream-Verschlüsselung RC4</u> zur <u>Vertraulichkeit</u> und die <u>Cyclic Redundancy Check-32</u> (CRC-32)-Prüfsumme zur <u>Integrität</u>.

Das standardmäßige 64-Bit-WEP verwendet einen <u>40-Bit-</u> Schlüssel (auch WEP-40 genannt), der zur

Bildung des RC4-Schlüssels mit einem 24-Bit-<u>Initialisierungsvektor (</u>IV) <u>verknüpft</u> wird. Ein 64-Bit-WEP-Schlüssel wird in der Regel als Zeichenfolge mit 10 <u>Hexadezimalzeichen (</u>Basis 16) (0 bis 9 und A-F) eingegeben. Jedes Zeichen steht für vier Bit, und zehn Ziffern von vier Bit entsprechen jeweils 40 Bit. Wenn Sie den 24-Bit-IV hinzufügen, wird der vollständige 64-Bit-WEP-Schlüssel erzeugt.

Ein 128-Bit-WEP-Schlüssel wird normalerweise als Zeichenfolge mit 26 Hexadezimalzeichen eingegeben. 26 Ziffern mit vier Bit entsprechen 104 Bit. Wenn Sie den 24-Bit-IV hinzufügen, wird der vollständige 128-Bit-WEP-Schlüssel erzeugt. Die meisten Geräte erlauben dem Benutzer, den Schlüssel als 13 ASCII-Zeichen einzugeben.

Authentifizierungsmethoden

Mit WEP können zwei Authentifizierungsmethoden verwendet werden: Open System Authentication und Shared Key Authentication.

Bei der offenen Systemauthentifizierung muss der WLAN-Client dem WAP keine Anmeldeinformationen für die Authentifizierung bereitstellen. Jeder Client kann sich beim Access Point authentifizieren und dann versuchen, eine Verbindung herzustellen. Im Prinzip findet keine Authentifizierung statt. Anschließend können WEP-Schlüssel verwendet werden, um Datenrahmen zu verschlüsseln. An dieser Stelle muss der Client über die richtigen Schlüssel verfügen.

Bei der Shared Key-Authentifizierung wird der WEP-Schlüssel für die Authentifizierung in einem vierstufigen Challenge-Response-Handshake verwendet:

- 1. Der Client sendet eine Authentifizierungsanforderung an den WAP.
- 2. Der Access Point antwortet mit einer <u>Klartext-</u> Herausforderung.
- 3. Der Client verschlüsselt den Abfragetext mit dem konfigurierten WEP-Schlüssel und antwortet mit einer weiteren Authentifizierungsanforderung.
- 4. Der WAP entschlüsselt die Antwort. Stimmt die Antwort mit dem Text der Herausforderung überein, sendet der Access Point eine positive Antwort.

Nach der Authentifizierung und Zuordnung wird auch der vorinstallierte WEP-Schlüssel verwendet, um die Datenframes mit RC4 zu verschlüsseln.

Auf den ersten Blick mag es so aussehen, als ob Shared Key Authentication sicherer ist als Open System Authentication, da letztere keine echte Authentifizierung bietet. Das Gegenteil ist jedoch der Fall. Es ist möglich, den für den Handshake verwendeten Schlüsselstrom abzuleiten, wenn Sie die Challenge-Frames in Shared Key Authentication erfassen. Daher ist es ratsam, für die WEP-Authentifizierung statt der Shared Key-Authentifizierung die Open System Authentication zu verwenden.

Das TKIP (Temporal Key Integrity Protocol) wurde erstellt, um diese WEP-Probleme zu beheben. Ähnlich wie WEP verwendet TKIP die RC4-Verschlüsselung. TKIP erweitert WEP jedoch um zusätzliche Maßnahmen wie paketbasiertes Key Hashing, Message Integrity Check (MIC) und Broadcast Key Rotation, um bekannte WEP-Schwachstellen zu beheben. TKIP verwendet die RC4-Stream-Verschlüsselung mit 128-Bit-Schlüsseln für die Verschlüsselung und 64-Bit-Schlüsseln für die Authentifizierung.

Konfigurieren

In diesem Abschnitt werden die GUI- und CLI-Konfigurationen für WEP beschrieben.

GUI-Konfiguration

Führen Sie diese Schritte aus, um WEP mit der GUI zu konfigurieren.

- 1. Stellen Sie über die Benutzeroberfläche eine Verbindung zum AP her.
- 2. Wählen Sie im Menü Security (Sicherheit) auf der linken Seite des Fensters für die Funkschnittstelle, für die Sie die statischen WEP-Schlüssel konfigurieren möchten, den Verschlüsselungs-Manager aus.
- 3. Klicken Sie unter Verschlüsselungsmodi auf **WEP-Verschlüsselung**, und wählen Sie **Obligatorisch** aus dem Dropdown-Menü für den Client aus.

Die von Station verwendeten Verschlüsselungsmodi sind:

- **Standard (keine Verschlüsselung)** Erfordert, dass Clients ohne Datenverschlüsselung mit dem Access Point kommunizieren. Diese Einstellung wird nicht empfohlen.
- **Optional** Ermöglicht Clients die Kommunikation mit dem Access Point entweder mit oder ohne Datenverschlüsselung. In der Regel verwenden Sie diese Option, wenn Clientgeräte vorhanden sind, die keine WEP-Verbindung herstellen können, z. B. Clients von anderen Anbietern in einer 128-Bit-WEP-Umgebung.
- **Obligatorisch (vollständige Verschlüsselung)** Erfordert, dass Clients Datenverschlüsselung verwenden, wenn sie mit dem WAP kommunizieren. Clients, die keine Datenverschlüsselung verwenden, dürfen nicht kommunizieren. Diese Option wird empfohlen, wenn Sie die Sicherheit Ihres WLAN maximieren möchten.
- 4. Wählen Sie unter Encryption Keys (Verschlüsselungsschlüssel) das Optionsfeld **Transmit Key** (**Übertragungsschlüssel**) aus, und geben Sie den zehnstelligen Hexadezimalschlüssel ein. Stellen Sie sicher, dass die Schlüsselgröße auf **40 Bit** festgelegt ist.

Geben Sie 10 Hexadezimalziffern für 40-Bit-WEP-Schlüssel oder 26 Hexadezimalziffern für 128-Bit-WEP-Schlüssel ein. Bei den Tasten kann es sich um eine beliebige Kombination der folgenden Ziffern handeln:

- 0 bis 9
- a bis f
- A bis F

cisco	HOME NETWORK ASSOCIATIO		SERVICES SOFTWARE E	иент L00	Saye Configuration Bing Logout		
Security	RADIO8-602.11%	24090	RADIO1-882.11N ^{56H2}				
Admin Access	Hostname ap				ap uptime is 3 hours, 41 minut		
Incryption Manager	Security: Encryption Manag	er - Radic0-802.11N ^{2.4GBr}					
SSID Manager Server Manager	Encryption Nodes						
AP Authentication	© None						
Intrusion Detection Local RADIUS Server	WEP Encryption	Mandalary *					
Advance Security			Cisco Compliant TKIP	Features 🛛 Enable Message Integrity Check (MC)			
	-			Enable Per Packet Keying (PPK)			
	© Cipher	WEP 128 bit	•				
	Encryption Keys						
			Transmit Key	Encryption Key (Hexadeoima)	Key Size		
		Encryption Key 1:	•	*******	40 bž 💌		
		Encryption Key 2:	0		128 bit +		
		Encryption Key 3:	0		128 bit =		
		Encryption Key 4:	0		128 bit -		

5. Klicken Sie auf **Apply-All** (Übernehmen), um die Konfiguration für beide Funkmodule anzuwenden.

Broadcast Key Rotation Interval:	Disable Rotation		
	Enable Rotation with Interval DISABLED (10-10000000 sec)		
WPA Group Key Update:	Enable Group Key Update On Membership Termination		
	Enable Group Key Update On Member's Capability Change		
		Acoly-Radia0	Apply-All

6. Erstellen Sie einen Service Set Identifier (SSID) mit **Open Authentication**, und klicken Sie auf **Apply**, um ihn für beide Funkmodule zu aktivieren.

				🟫 🖛 😋 🔜 🖬 🖬 Tabao	Ρ 🖡 1			
					Sage Configuration Bing Logout			
HOME P	ETWORK ASSOCIATION	A MIDELESS SECONDA BBANI	CES SOFTWARE EVENTLOG					
Heste					ap uptime is 3 hours, 45 min			
Sec	vity: Global SSID Manage	**						
550	Properties							
6 1	and PPID I he							
Cur Ca			550-	and seeling				
	a-cantig		VLAN	< NONE > * Defects the				
			TERM.	Backap 1:				
		-		Backap 2				
			Band Salad	Becksp 2				
			beno-orient.	Band Select Band Select Z 45Hz				
				Radio0-302.11NP 044				
			Network ID:	(D-4096)				
D	alata							
Cier	Client Authoritics Settings							
	Matheaster Association							
	Mathods Accepted	1:		7				
	Nethods Accepted	e uthentication	< NO ADDITION> +]				
	Nethods Accepted	e: uthentication: Authentication:	< NO ADDITION> • < NO ADDITION> •	ב				
	Nethods Accepted	8: uthertication: Authentication:	< NO ADDITION> • < NO ADDITION> •	3				
	Nethods Accepted	£ uthertication Authertication	< NO ADDITION> • < NO ADDITION> •]				
	Methods Accepted	8 athentication Authentication	< NO ADDITION> -	כ				
	Nethoda Accepted	8: uthentication: Authentication:	< NO ADDITION> •]				
Guest M	Nethoda Accepter Copen A Stared odefinificationchare SBD 5	t: uthenscation Authenscation Authenscation	< NO ADDITION> •]				
Guest M	Nethoda Accepter	t: uthentscation Authentication Authentication	< NO ADDITION> • < NO ADDITION> •]				
Guest M Radioŭ Set Be	Nethods Accepter Copen A Copen A Stered odefinitestructure SBD 5 ecc. 1116 ^{2,4000} ; ecce Mode:	t: athentication Authentication Westings Windje BSSD Set Sm	< NO ADDITION> • < NO ADDITION> • ge Geest Mode SSD wep-config •]				
Guest M Radiaŭ Set Be	Nethoda Accepter Copen A Stand odefinificationcture SBID S ecc. Http2: AGRs; ecc. Mode:	t: athentication Authentication Settings Sangle BSSD Set Sm Onutiple BSSD Set Sm	< NO ADDITION> • < NO ADDITION> • gle Gaest Mode SSD wep-cardig •]				
Guest M Radioŭ Set Be Set Int	Nethoda Accepter Quera A Strend odefinifestructure SSID S acce Mode: acce Mode: astructure SSID:	t: athentication: Authentication: Writings Writings Writings Writings C NORE > + ESSD C NORE > + Escourt	KIO ADDITION>					
Guest M Radio0 Set Be Set Int	Nethoda Accepter Open A Shared Shared Accepter Shared Accepter Accepter Shared Accepter Accepter Accepter Shared Accepter A	t: athentication: Authentication Authentication Bettings Bragie BSSID Set Sim Watepie BSSID < NONE > • T Force int	KIO ADDITION>	_				
Guest M Radioŭ Set Be Set Inh Radio 1 Set Be	Nethoda Accepter Copen A Shared Shared Acception	t: athentication: Authentication: Authentication: Sectings: Sectings: Secting:	KIO ADDITION>	_				
Guest M RadioC Set Be Set Im Radio1 Set Be	Nethoda Accepter Control Control Shared Accentrol A	t: athentication: Authentication: initiage initiage Multiple BSSD Set Sin Note PSSD Set Sin Note PSSD Set Sin Note PSSD Set Sin Note PSSD Set Sin	KIO ADDITION>]				
Guest M Radio0 Set Be Set Int Radio1 Set Be Set Int	Nethoda Accepter Open A Steered Steered Steered Accentry Ac	E athentication: Authentication: Hettings] ,				
Guest M RadioD Set Be Set Int Radio1 Set Int	Nethoda Accepter Control of the second Strend odefinitestructure SSID 5 acce Mode: acce Mode: ac	E athentication: Authentication: Hettings Single BSSID Set Sin Number BSSID C NONE > • Force int Number BSSID C NONE > • Force int	KIO ADDITION> C NO ADDITION C NO ADD]				

7. Navigieren Sie zum Netzwerk, und aktivieren Sie die Funkmodule für **2,4 GHz** und **5 GHz**, um sie in Betrieb zu nehmen.

CLI-Konfiguration

In diesem Abschnitt können Sie WEP mit der CLI konfigurieren.

```
ap#
```

show run

```
Building configuration...
Current configuration : 1794 bytes
Т
Т
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname ap
!
I
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
ļ
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
  dot11 ssid wep-config
  authentication open
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
1
1
bridge irb
1
!
ļ
interface Dot11Radio0
no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 1
 antenna gain 0
 station-role root
 bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
I
interface Dot11Radio1
```

```
no ip address
 1
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 ssid wep-config
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
ļ
interface GigabitEthernet0
no ip address
 duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
I
interface BVI1
ip address dhcp
1
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
bridge 1 route ip
!
!
1
line con 0
line vty 0 4
login local
transport input all
1
end
```

Überprüfung

Geben Sie den folgenden Befehl ein, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert:

<#root>

ap#

show dot11 associations

802.11 Client St	tations on Dot1	1Radio0:			
SSID [wep-config	g] :				
MAC Address	IP address	Device	Name	Parent	State
1cb0.94a2.f64c	10.106.127.251	unknown	-	self	Assoc

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um Probleme mit Ihrer Konfiguration zu beheben.

Hinweis: Lesen Sie <u>Wichtige Informationen</u> zu <u>Debug-Befehlen</u>, bevor Sie **Debug-**Befehle verwenden.

Die folgenden Debug-Befehle sind nützlich, um Fehler in der Konfiguration zu beheben:

- debug dot11 events: Aktiviert das Debugging für alle dot1x-Ereignisse.
- **debug dot11-Pakete**: Aktiviert das Debugging für alle dot1x-Pakete.

Das folgende Beispiel wird angezeigt, wenn der Client erfolgreich eine Verbindung mit dem WLAN herstellt:

*Mar 1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 1cb0.94a2.f64c Associated KEY_MGMT[NONE]

Wenn der Client den falschen Schlüssel eingibt, wird folgender Fehler angezeigt:

*Mar 1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c *Mar 1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 1cb0.94a2.f64c Reason: Sending station has left the BSS *Mar 1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.