Configuratie van EFG op Aironet access points en bruggen

Inhoud

Inleiding

Dit document biedt methoden om bekabelde equivalente Privacy (EFN) te configureren op Cisco Aironet draadloze LAN-componenten (WLAN).

N.B.: Raadpleeg het gedeelte Static Web Keys van Hoofdstuk 6 - WLAN's configureren voor meer informatie over de formatie van EFG op draadloze LAN-controllers (WLC's).

Het encryptie-algoritme is ingebouwd in de 802.11 (Wi-Fi) standaard. Codering gebruikt de code 4 (RC4) van de Ron stream met 40- of 104-bits toetsen en een 24-bits initialisatiedrager (IV).

Zoals de standaard specificeert, gebruikt EFG het RC4-algoritme met een 40-bits of 104-bits toets en een 24-bits IV. RC4 is een symmetrisch algoritme omdat het dezelfde sleutel voor de encryptie en de decryptie van gegevens gebruikt. Wanneer de verbinding van de radio wordt geactiveerd, heeft elk "station" een sleutel. De toets wordt gebruikt om de gegevens te vervormen voordat de gegevens via de ether worden doorgegeven. Als een station een pakje ontvangt dat niet met de juiste sleutel is bebouwd, wordt het pakje verworpen en nooit aan de host geleverd.

De voorkeur kan in eerste instantie worden gegeven aan een thuiskantoor of een klein kantoor dat geen zeer sterke beveiliging vereist.

De implementatie van Aironet de tenuitvoerlegging van het EFG bevindt zich in de hardware. Daarom zijn er minimale resultaten voor de impact van de prestaties als u gebruikmaakt van de code.

Opmerking: Er zijn een aantal bekende problemen met behulp van de code-code-code-code-code, waardoor de code geen sterke coderingsmethode is. Het gaat hierbij om:

- Er is veel administratieve overheadkosten om een gedeelde sleutel van de EVN te handhaven.
- De code van het gebruik van het gebruik van het gebruik van het gebruik van het apparaat is gebaseerd op het gebruik van het apparaat. Elk geheim dat aan één persoon wordt gegeven, wordt openbaar na een periode.
- De IV die het algoritme van de EVN zaait wordt in duidelijke tekst verzonden.
- De de checksum van de tolk is lineair en voorspelbaar.

TKIP (Temporal Key Integrity Protocol) is gecreëerd om deze problemen met EFG aan te pakken. Gelijkaardig aan NUL gebruikt TKIP RC4-encryptie. TKIP verbetert echter EFG door maatregelen toe te voegen zoals hashing per pakket, Berichtintegriteitscontrole (MIC) en Broadcast-sleutelrotatie om bekende kwetsbaarheden van EVN aan te pakken. TKIP gebruikt een RC4-stream algoritme met 128-bits coderingen en 64-bits coderingen voor verificatie.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat u een administratieve verbinding met de WLAN-apparaten kunt maken en dat de apparaten normaal in een niet-versleutelde omgeving werken.

Om de standaard 40-bits EFN te configureren moet u twee of meer radio-eenheden hebben die met elkaar communiceren.

Opmerking: De Aironet-producten kunnen 40-bits Gigabit-verbindingen maken met IEEE 802.11b-conforme niet-Cisco-producten. Dit document heeft geen betrekking op de configuratie van andere apparaten.

Voor het maken van een 128-bits verbinding met draadloos WAN, werken Cisco-producten alleen in interactie met andere Cisco-producten.

Gebruikte componenten

Gebruik deze onderdelen in dit document:

- Twee of meer radioeenheden die met elkaar communiceren
- Een beheerverbinding met het WLAN-apparaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

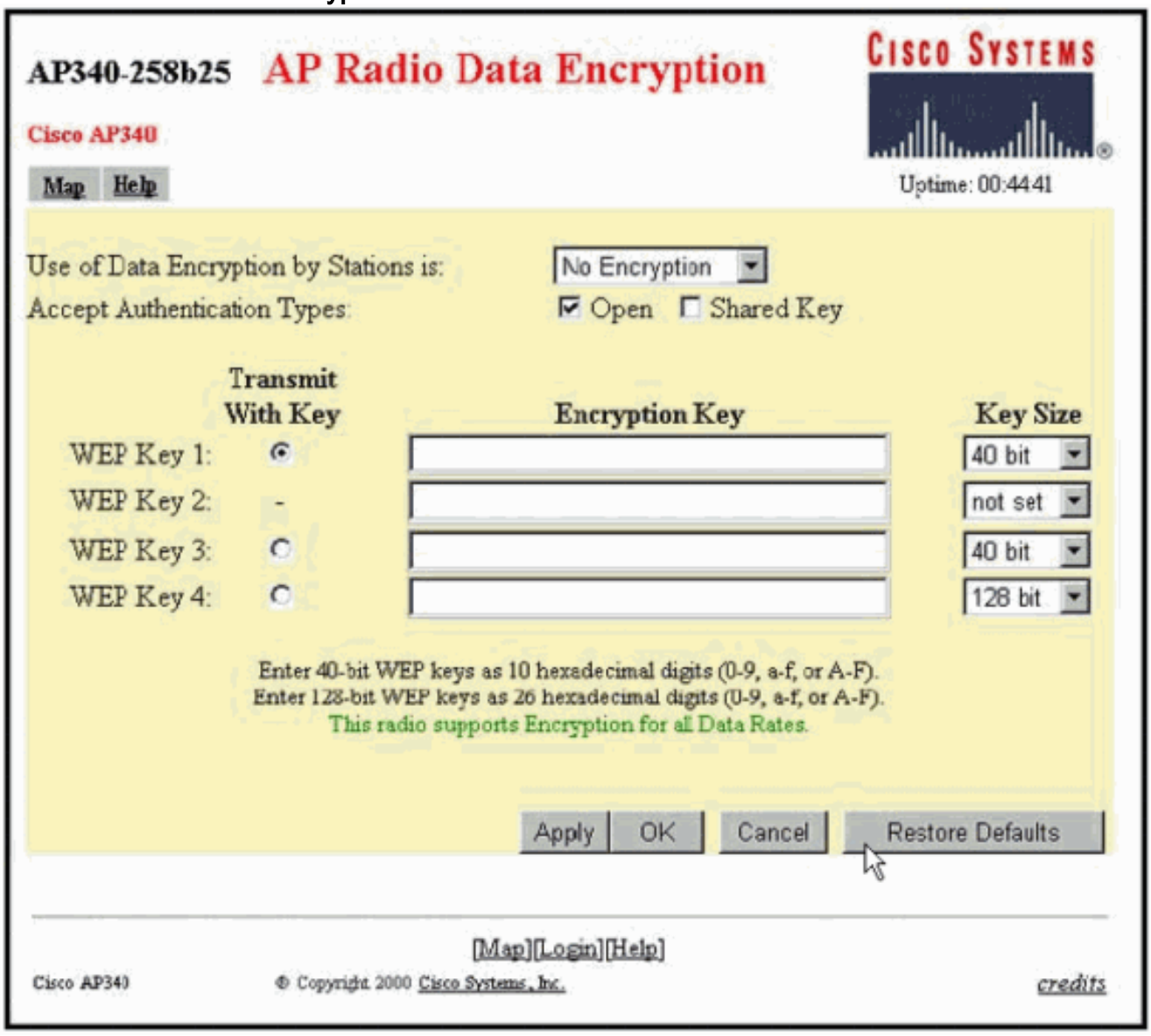
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Wireless-N access points voor Aironet configureren

Aironet access points voor gebruik van VXWorks

Voer de volgende stappen uit:

1. Maak een verbinding met het access point (AP).
2. Navigeer naar het menu AP Radio Encryption.Gebruik een van deze paden:**Summary Status > Setup > AP Radio/Hardware > Radio Data Encryption (EFG) > AP Radio Data EncryptionSummary Status > Setup > Security > Security Setup: Radio Data Encryption (EFN) > AP Radio Data EncryptionN.B.:** Als u wijzigingen in deze pagina wilt aanbrengen, moet u een beheerder met de functies Identity en Schrijven zijn.**Web browser View van het menu AP Radio Data Encryption**



Instellingen VXWorks

De pagina met AP Radio Data Encryption bevat een verscheidenheid aan te gebruiken opties.

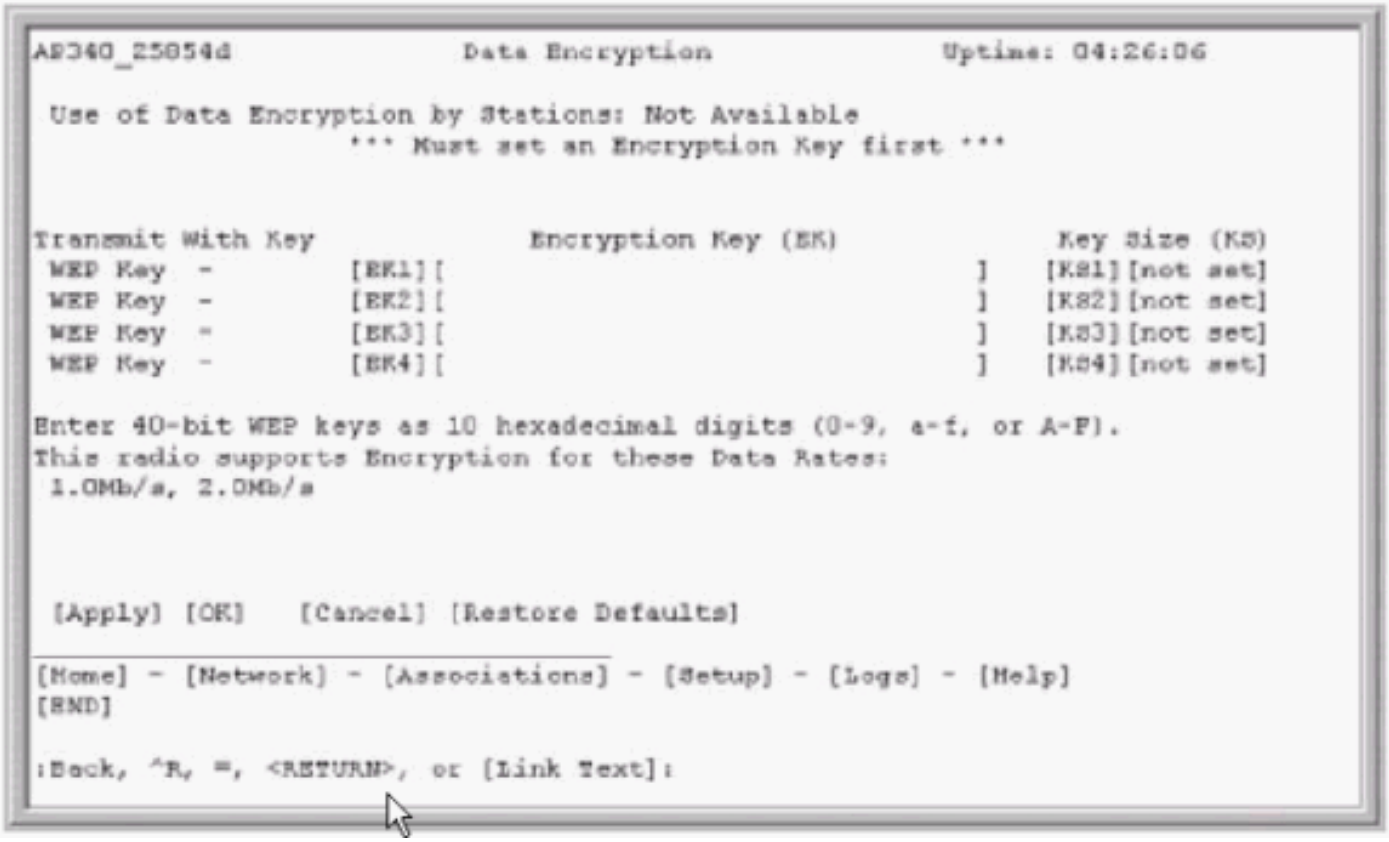
Sommige opties zijn verplicht voor het gebruik van een bepaalde code. In deze paragraaf worden deze verplichte opties vermeld. Andere opties zijn niet nodig voor de functie van medegebruik, maar ze worden aanbevolen.

- **Het gebruik van gegevensencryptie door Stations is:**Gebruik deze instelling om te kiezen of klanten gegevensencryptie moeten gebruiken wanneer ze met AP communiceren. Het Pull-Down-menu bevat drie opties:**Geen encryptie (standaard)** - vereist dat klanten met AP communiceren zonder enige gegevensencryptie. Deze instelling wordt niet aanbevolen.**Facultatief**-staat componenten toe om met AP met of zonder gegevensencryptie te communiceren. Meestal gebruikt u deze optie wanneer u clientapparaten hebt die geen verbinding met een netwerk kunnen maken zoals niet-Cisco-clients in een 128-bits EFN-omgeving.**Full Encryption (AANBEVOLEN)** - vereist dat de cliënten gegevensencryptie gebruiken wanneer zij met AP communiceren. Clients die geen gegevensencryptie gebruiken, mogen niet communiceren. Deze optie wordt aanbevolen als u de beveiliging van uw WLAN wilt maximaliseren.**Opmerking:** U moet een de sleutel van de EVN instellen voordat u coderingsgebruik toelaat. Raadpleeg het gedeelte **Encryption Key (MANDATORY)** van deze lijst.
- **Verificatietypen accepteren**U kunt Open, Shared Key of beide opties kiezen om de authenticaties in te stellen die het AP zal herkennen.**Open (AANBEVOLEN)** - Deze standaardinstelling maakt het mogelijk dat een apparaat, ongeacht de sleutels van de EVN, authenticeert en probeert te associëren.**Gedeelde sleutel**-Deze instelling vertelt AP om een platte tekst, gedeelde zeer belangrijke vraag naar elk apparaat te verzenden dat met AP probeert te associëren.**Opmerking:** Deze query kan AP openlaten voor een bekende tekstaanval van indringers. Daarom is deze instelling niet zo veilig als de instelling Open.
- **Verzenden met sleutel**Met deze knoppen kunt u de toets selecteren die het AP tijdens gegevensoverdracht gebruikt. U kunt slechts één toets tegelijkertijd selecteren. Alle ingestelde toetsen kunnen worden gebruikt om gegevens te ontvangen. U dient de toets in te stellen voordat u deze als de verzendtoets specificeert.
- **Versleutel tot versleuteling (VERPLICHT)**Deze velden staan u toe om de sleutels van de EVN in te voeren. Voer 10 hexadecimale cijfers in voor 40-bits EFN-toetsen of 26 hexadecimale cijfers voor 128-bits EFN-toetsen. De toetsen kunnen worden gebruikt door een combinatie van deze cijfers:0 tot 9a tot fA tot FOm de zeer belangrijke veiligheid van EFN te beschermen, verschijnen de bestaande sleutels van EFN niet in onduidelijke tekst in de ingangsvelden. In recente versies van APs, kunt u bestaande sleutels wissen. U kunt de bestaande toetsen echter niet bewerken.**Opmerking:** u moet de de sleutels van de EVN voor uw netwerk, APs, en clientapparaten op precies dezelfde manier instellen. Bijvoorbeeld, als u de sleutel van de sleutel 3 van de EVN op uw AP aan 0987654321 instelt en deze sleutel als de actieve sleutel selecteert, moet u ook de sleutel van de sleutel van de Gebruiker 3 op het clientapparaat aan de zelfde waarde instellen.
- **Sleutelgrootte (VERPLICHT)**Deze instelling stelt de toetsen in op 40-bits of 128-bits EFN. Als "not set" voor deze selectie wordt weergegeven, wordt de toets niet ingesteld.**Opmerking:** u kunt een toets niet verwijderen door "not set" te selecteren.
- **Actieknoppen**Vier bedieningsinstellingen. Als JavaScript op uw webbrowser is ingeschakeld, verschijnt een bevestigingsvenster nadat u op een willekeurige knop klikt, behalve Annuleren.**Toepassen** - Met deze knop wordt de nieuwe waardinstellingen geactiveerd. De browser blijft op de pagina staan.**OK** - Deze knop past de nieuwe instellingen toe en beweegt de browser terug naar de hoofdpagina met de instellingen.**Annuleren** - Met deze knop wordt de instelling van wijzigingen geannuleerd en worden de eerder opgeslagen waarden hersteld.

U keert dan terug naar de hoofdpagina met de instellingen.**Standaardinstellingen herstellen** - Met deze knop worden alle instellingen op deze pagina hersteld naar de standaardinstellingen van de fabriek.

Opmerking: In recente Cisco IOS® versies van APs **zijn** alleen de knoppen **Toepassen** en **Annuleren** beschikbaar voor deze pagina.

Terminalweergave van het menu Gegevensversleuteling



Terminalsimulator weergave van de sleutel van de EVN Configuration Sequence (Cisco IOS®-software)

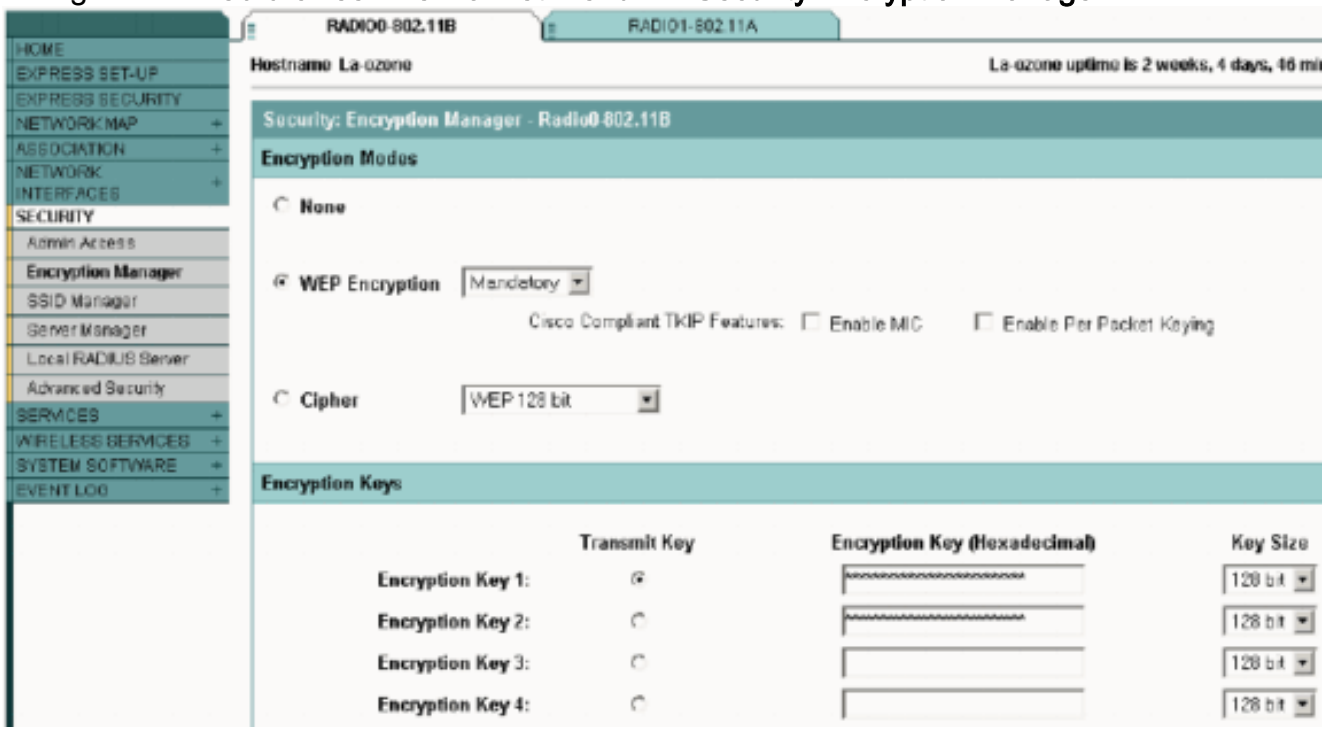
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
  transmit-key  Set the key as transmit key
  <cr>

La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee transmit-key
La-ozone(config-if)#end
La-ozone#
*Mar 19 00:42:13.893: %SYS-5-CONFIG_I: Configured from console by console
La-ozone#
La-ozone#
```

Aironet APs die Cisco IOS software uitvoeren

Voer de volgende stappen uit:

1. Maak een verbinding met de AP.
2. Kies in het menu BEVEILIGING aan de linkerkant van het venster de optie **Encryption**

Manager voor de radio-interface waaraan u de statische toetsen van EFG wilt configureren.**Web browser View of het menu AP Security Encryption Manager**



Aironet bruggen configureren

Als u VxWorks gebruikt, voert u deze stappen uit:

1. Maak een verbinding met de brug.
2. Blader naar het Privacymenu.Kies **het hoofdmenu > Configuratie > Radio > I80211 > Privacy**.Het Privacymenu regelt het gebruik van encryptie op het gegevenspakket dat door de radio's over de lucht wordt verzonden. Het RSA RC4-algoritme en een van maximaal vier bekende toetsen worden gebruikt om de pakketten te versleutelen. Elk knooppunt in de radiocel moet alle gebruikte toetsen kennen, maar een van de toetsen kan worden geselecteerd om de gegevens te verzenden.**Terminalweergave van het Privacymenu**

```
        Configuration Radio I80211 Privacy Menu
     Option          Value       Description
1 - Encryption    [ off  ]    - Encrypt radio packets
2 - Auth          [ open ]    - Authentication mode
3 - Client        [ open ]    - Client authentication modes allowed
4 - Key                       - Set the keys
5 - Transmit                  - Key number for transmit
 Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

Raadpleeg Cipr-uitgangen en EFN configureren - 1300 Series brug en de eigenschappen van EFN en EFN configureren - 1400 Series brug voor informatie over de manier waarop u EFN kunt configureren in 1300 en 1400 Series bruggen door CLI-modus.

Om GUI te gebruiken om 1300 en 1400 Series bruggen te configureren voltooien de zelfde procedure die in Aironet AP's wordt uitgelegd die de sectie van Cisco IOS-software van dit document uitvoeren.

Instellingen VXWorks

Het Privacymenu bevat een aantal opties die u moet configureren. Sommige opties zijn verplicht voor het gebruik van een bepaalde code. In deze paragraaf worden deze verplichte opties vermeld. Andere opties zijn niet nodig voor de functie van medegebruik, maar ze worden aanbevolen.

In deze sectie worden de menu-opties weergegeven in de volgorde waarin ze verschijnen in de terminalweergave van het Privacymenu. Configureer de opties in deze volgorde:

1. Sleutel
2. zenden
3. Auth
4. Clientclient
5. Versleuteling

De configuratie in deze volgorde zorgt ervoor dat de gewenste voorwaarden worden ingesteld terwijl u elke instelling configureren.

Dit zijn de opties:

- **Sleutel (VERPLICHT)**De Key optie programmeert de encryptiesleutels in de Bridge. U wordt gevraagd een van de vier toetsen in te stellen. U wordt twee keer gevraagd de toets in te voeren. Om de sleutel te definiëren, moet u of 10 of 26 hexadecimale cijfers invoeren, die afhangen van of de configuratie van de Brug voor 40 bit of 128-bits toetsen is. Gebruik een combinatie van deze cijfers:0 tot 9a tot fA tot FDe toetsen moeten overeenkomen in ***alle knooppunten in de radiocel en u moet de toetsen in dezelfde volgorde invoeren.*** U hoeft niet alle vier toetsen te definiëren, zolang het aantal toetsen in elk apparaat in de WLAN-functie voorkomt.
- **zenden**De optie Verzenden vertelt de radio welke toetsen gebruikt moeten worden om pakketten te verzenden. Elke radio kan ontvangen pakketten decrypteren die met om het even welke van de vier sleutels worden verzonden.
- **Auth**U gebruikt de optie Auth op repeaterbruggen om te bepalen welke authenticatiemodus de unit gebruikt om verbinding te maken met de parent. De toegestane waarden zijn Open of Shared Key. Het protocol 802.11 specificeert een procedure waarin een client voor authenticatie met een ouder moet zijn voordat de client een andere client kan gebruiken.**Open (AANBEVOLEN)** - Deze wijze van authenticatie is in wezen een nul operatie. Alle klanten mogen authentiek zijn.**Shared Key**-Deze modus staat de ouder toe om de client een uitdagingstekst te verzenden, die de client versleutelt en naar de parent terugkeert. Als de ouder de challenge tekst met succes decrypteert, wordt de client echt bevonden.**Waarschuwing:** gebruik de gedeelde sleutel niet. Wanneer u het gebruikt, wordt er in de lucht een gewone tekst en een gecodeerde versie van dezelfde gegevens verzonden. Dit heeft niets aan te merken. Als de gebruikerstoets fout is, decrypteert de unit de pakketten niet en kunnen de pakketten geen toegang tot het netwerk verkrijgen.
- **Clientclient**De clientoptie bepaalt de verificatiemodus die de clientknooppunten gebruiken om de eenheid aan te sluiten. Dit zijn de toegestane waarden:**Open (AANBEVOLEN)** - Deze wijze van authenticatie is in wezen een nul operatie. Alle klanten mogen authentiek zijn.**Shared Key**-Deze modus staat de ouder toe om de client een uitdagingstekst te verzenden, die de client versleutelt en naar de parent terugkeert. Als de ouder de challenge tekst met succes decrypteert, wordt de client echt bevonden.**Beide**—in deze modus kan de client beide modi

gebruiken.

- **VersleutelingUit** - Als u de optie Encryptie op Off instelt, wordt er geen encryptie uitgevoerd. Gegevens verzenden in de duidelijke taal.**Op (VERPLICHT)** - Als u de optie Encryptie op On instelt, worden alle verzonden gegevens versleuteld en worden alle niet-versleutelde ontvangen pakketten verwijderd.**Gemengde**—In de Gemengde modus accepteert een wortel of repeater brug associatie van klanten die encryptie aan of Uit hebben ingeschakeld. In dit geval worden alleen gegevenspakketten tussen knooppunten versleuteld die beide ondersteuning bieden. Multicastpakketten worden in de vrije ruimte verzonden. Alle knooppunten kunnen de pakketten zien.**Waarschuwing:** gebruik de gemengde modus niet. Als een client met encryptie een multicast pakje naar de parent verstuurt, is het pakket versleuteld. De ouder decrypteert het pakje en geeft het pakje in het helder over naar de cel, en andere knooppunten kunnen het pakje zien. De mogelijkheid om een pakket in zowel gecodeerde als niet-gecodeerde formulieren te bekijken kan bijdragen aan het breken van een sleutel. De optie Gemengde modus is alleen ingebouwd voor compatibiliteit met andere leveranciers.

Clientadapters configureren

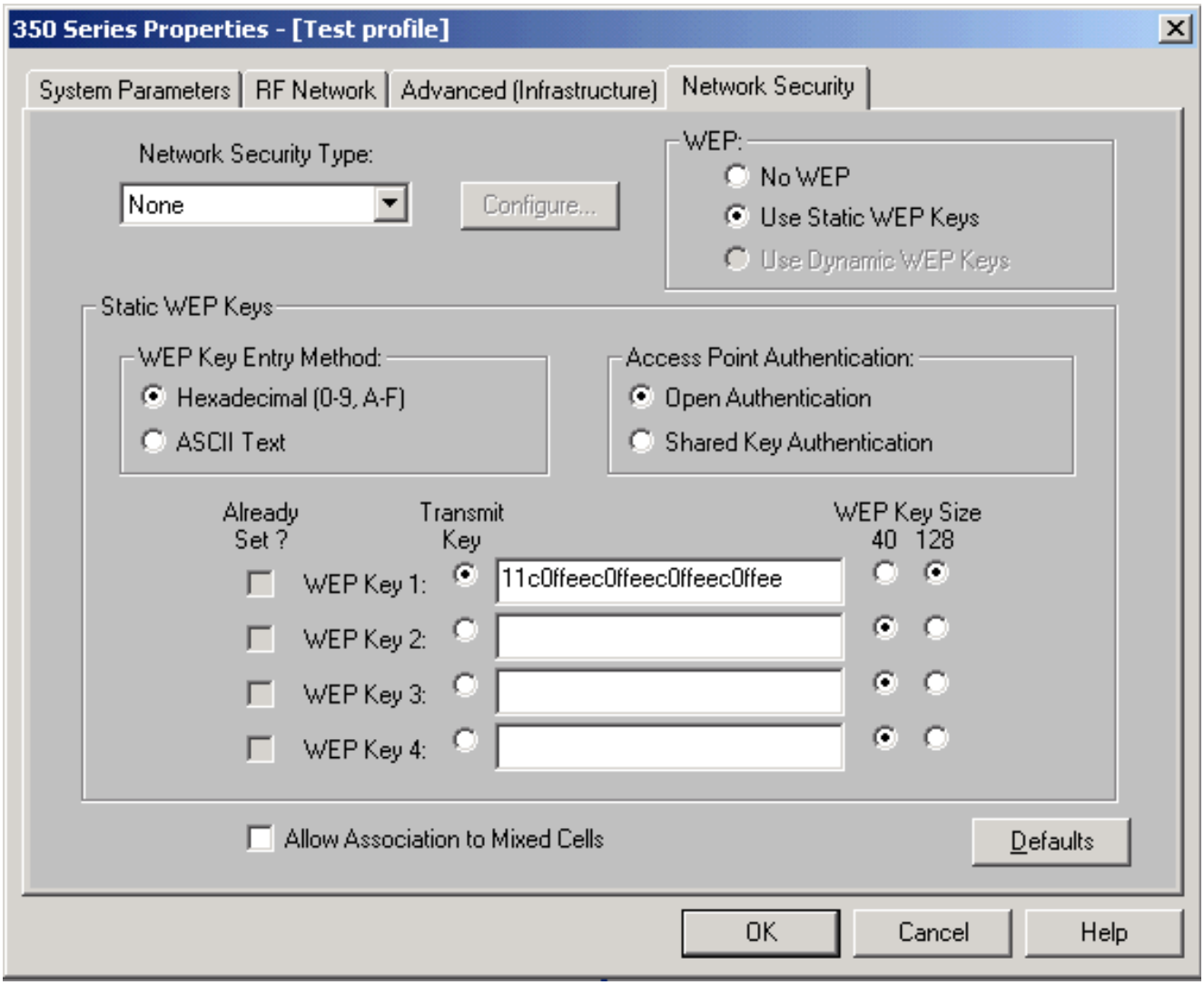
U moet twee hoofdstappen voltooien om het gebruik van NUL op de Aironet-clientadapter in te stellen:

1. Configuratie van de sleutel/de sleutels van de EVN in de Manager van de Versleuteling van de client.
2. Schakel EFN in het Aironet Client Utility (ACU) in.

Stel de EFN-toetsen in

Voltooi deze stappen om de knoppen van de client op het gebruik van een wiel te zetten:

1. Open ACU en kies **Profile Manager**.
2. Kies het profiel waar u EFN wilt inschakelen en klik op **Bewerken**.
3. Klik op het tabblad **Netwerkbeveiliging** om de beveiligingsopties weer te geven en klik op **Statische EFN-toetsen gebruiken**.Deze actie activeert de de configuratieopties van EFG die worden gedimd wanneer geen anti-EGN wordt geselecteerd.



4. Voor de de sleutel van de EVN die u wilt creëren, kies of **40** bits of **128** bits onder de sleutel van de Maat van **de** sleutel van **de** EVN aan de rechterkant van het venster.**Opmerking:** Clientadapters met 128 bits kunnen 40 bits of 128 bits gebruiken. Maar 40-bits adapters kunnen alleen 40-bits toetsen gebruiken.**Opmerking:** Uw client-adapter-sleutel moet overeenkomen met de EFN-toets die de andere WLAN-componenten bevat waarmee u gebruik overbrengt.Wanneer u meer dan één de sleutel van EFN instelt, moet u de sleutels van de EVN aan de zelfde de sleutelnummers van de EVN voor alle apparaten toewijzen. De sleutels van EFG moeten uit de hexadecimale tekens samengesteld zijn en moeten 10 tekens bevatten voor 40 bit - de sleutels van EFN of 26 tekens voor 128-bits de sleutels van EFN. De hexadecimale tekens kunnen zijn:0 tot 9a tot fA tot F**Opmerking:** de toetsen ASCII-tekst van het EFN worden niet ondersteund op Aironet APs. Daarom moet u de optie Hexadecimaal (0-9, A-F) kiezen als u van plan bent uw clientadapter met deze AP's te gebruiken.**Opmerking:** Nadat u de sleutel van het EFN maakt, kunt u erover schrijven. Maar u kunt het niet bewerken of verwijderen.**Opmerking:** Als u een latere versie van Aironet Desktop Utility (ADU) in plaats van ACU gebruikt als clienthulpprogramma, kunt u ook de gemaakte EFN-toets verwijderen en vervangen door een nieuwe.
5. Klik op de knop **Verzenden** naast een van de toetsen die u hebt gemaakt.Met deze actie geeft u aan dat deze toets de toets is die u wilt gebruiken om pakketten te verzenden.
6. Klik op **Persistent** onder het sleuteltype van EFG.Met deze actie kan de clientadapter deze de sleutel van de EVN bewaren, zelfs wanneer de stroom naar de adapter wordt verwijderd of bij herstart van de computer waarin de sleutel is geïnstalleerd. Als u tijdelijk voor deze optie kiest, wordt de de sleutel van de EVN verloren wanneer de macht van uw clientadapter

wordt verwijderd.
7. Klik op **OK**.

Maakt gebruiken mogelijk

Voer de volgende stappen uit:

1. Open ACU en kies **Eigenschappen** in het menu.
2. Klik op het tabblad **Netwerkbeveiliging** om de beveiligingsopties weer te geven.
3. Controleer het aanvinkvakje **voorkomen** van **medegebruik** om medegebruik in te schakelen om het gebruik van de **modus** te activeren.

Raadpleeg het configureren van medegebruik in ADU voor stappen om medegebruik te configureren met behulp van ADU als clienthulpprogramma.

Werkgroepbruggen configureren

Er zijn verschillen tussen de Aironet 340 Series Workgroup Bridge en Aironet 340 Series Bridge. De configuratie van de werkgroepbridge voor het gebruik van EFN is echter vrijwel identiek aan de configuratie van de brug. Zie het gedeelte Aironet bruggen configureren voor het configureren van de brug.

1. Connect met de werkgroepbridge.
2. Blader naar het Privacymenu.Kies **Hoofdvenster > Configuration > Radio > I80211 > Privacy** om toegang te krijgen tot het menu Privacy VxWorks.

Instellingen

In het Privacymenu worden de instellingen weergegeven die in deze sectie worden weergegeven. Configureer de opties op de werkgroepbrug in deze volgorde:

1. Sleutel
2. zenden
3. Auth
4. Versleuteling

Dit zijn de opties:

- **Sleutel**De Belangrijkste optie bepaalt de sleutel van de EVN die de brug gebruikt om pakketten te ontvangen. De waarde moet overeenkomen met de toets die AP of ander apparaat waarmee de Workgroup Bridge het gebruik communiceert. De sleutel bestaat uit maximaal 10 hexadecimale tekens voor 40-bits codering of 26 hexadecimale tekens voor 128-bits codering. De hexadecimale tekens kunnen een combinatie van deze cijfers zijn:0 tot 9a tot fA tot F
- **zenden**De optie Verzenden bepaalt de de sleutel van EFN die de brug gebruikt om pakketten te verzenden. U kunt ervoor kiezen dezelfde toets te gebruiken als die u voor de Key optie hebt gebruikt. Als u een andere toets kiest, moet u een bijbehorende toets op het AP instellen.Er kan slechts één sleutel van EFG tegelijk worden gebruikt voor transmissies. De de sleutel van EFN die u gebruikt om gegevens over te brengen moet aan de zelfde waarde op uw Brug van de Werkgroep en andere apparaten worden geplaatst waarmee het

communiceert.

- **Verificatie (augustus)**De Auth parameter bepaalt welke methode van authenticatie het systeem gebruikt. De opties zijn:**Open (AANBEVOLEN)** - De standaard Open instelling stelt elke AP, ongeacht de instellingen van de EVN, in staat om authentiek te verklaren en dan te proberen met de brug te communiceren.**Gedeelde sleutel**—Deze instelling geeft de brug op een platte tekst, gedeelde zeer belangrijke vraag naar APs te verzenden in een poging om met de brug te communiceren. De gedeelde sleutel instelling kan de brug open laten voor een bekende aanslag van indringers. Daarom is deze instelling niet zo veilig als de instelling Open.
- **Versleuteling**Met de optie Encryptie worden encryptie-parameters op alle gegevenspakketten ingesteld, met uitzondering van associatiepakketten en bepaalde controlepakketten. Er zijn vier opties:**Opmerking:** AP moet encryptie actief hebben en een sleutel moet goed ingesteld worden.**Uit**: dit is de standaardinstelling. Alle encryptie is uitgeschakeld. De werkgroepbridge communiceert niet met een AP met gebruik van NUL.**Op (AANBEVOLEN)**—Voor deze instelling is de codering van alle gegevensoverdrachten vereist. De werkgroepbrug communiceert alleen met APs die gebruikmaken van EFG.**Gemengde op** - Deze instelling betekent dat de brug altijd gebruikt om met AP te communiceren. AP communiceert echter met alle apparaten, of zij gebruikt of niet gebruikt EFN.**Gemengde off**-Deze instelling betekent dat de brug geen gebruikmaakt van EFG om met AP te communiceren. AP communiceert echter met alle apparaten, of zij gebruikt of niet gebruikt EFN.**Waarschuwing:** Als u op of Gemengde op selecteert als de categorie van de EVN en u de brug door zijn radioverbinding vormt, wordt de verbinding aan de brug verloren als u de sleutel van de EVN verkeerd instelt. Zorg ervoor dat u precies de zelfde instellingen gebruikt wanneer u de de sleutel van EVN op de Werkgroepbridge en de sleutel van EVN op andere apparaten op uw WLAN instelt.

Gerelateerde informatie

- IEEE Standards Association
- Aironet 340 Series draadloze LAN-producten
- Draadloze ondersteuningsresources
- Draadloze LAN-ondersteuningspagina
- Cisco IOS-softwarerelease voor Cisco Aironet access points
- Cisco IOS-softwarerelease 1300 Series access point/brug voor buitengebruik
- Cisco Aironet access point softwareconfiguratie voor VXWorks
- Cisco Aironet 1400 Series brug-softwareconfiguratie
- Cisco Aironet draadloos LAN-clientadapterhandleidingen
- Cisco Wireless LAN-beveiligingsOverzicht
- Draadloos (mobiliteit) Beveiliging van draadloze netwerken
- Toegangspunt als voorbeeld voor een werkgroepbridge
- Cisco Aironet werkgroepbridge-Q
- Wachtwoordherstelprocedure voor Cisco Aironet-apparatuur
- Cisco Aironet access point QQ
- Technische ondersteuning en documentatie – Cisco Systems