Tipps zur Fehlerbehebung beim LWAPP-Upgrade-Tool

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Upgrade-Prozess - Übersicht
Upgrade-Tool - Grundlegender Betrieb
Wichtige Hinweise
Arten von Zertifikaten
Problem
Symptom
Lösungen
Ursache 1
Ursache 2
Ursache 3
Ursache 4
Ursache 5
Ursache 6
Ursache 7
Ursache 8
Tipps zur Fehlerbehebung
Zugehörige Informationen

Einführung

In diesem Dokument werden einige der wichtigsten Probleme erläutert, die auftreten können, wenn Sie das Upgrade-Tool zum Upgrade von autonomen Access Points (APs) auf den Lightweight-Modus verwenden. Dieses Dokument enthält auch Informationen darüber, wie diese Probleme behoben werden können.

Voraussetzungen

Anforderungen

APs müssen die Cisco IOS® Software Version 12.3(7)JA oder höher ausführen, bevor Sie das Upgrade durchführen können.

Cisco Controller müssen mindestens Softwareversion 3.1 ausführen.

Das Cisco Wireless Control System (WCS) (falls verwendet) muss mindestens Version 3.1 ausführen.

Das Aktualisierungsprogramm wird auf den Plattformen Windows 2000 und Windows XP unterstützt. Es muss eine dieser Windows-Betriebssystemversionen verwendet werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf diesen Access Points und Wireless LAN-Controllern.

Die APs, die diese Migration unterstützen, sind:

- Alle 1121G Access Points
- Alle Access Points der Serie 1130AG
- Alle Access Points der Serie 1240AG
- Alle Access Points der Serie 1250
- Bei allen IOS-basierten modularen Access Points der Serie 1200 (1200/1220 Cisco IOS Software Upgrade, 1210 und 1230 AP)-Plattformen ist Folgendes von der Funkeinheit abhängig:Wenn 802.11G, MP21G und MP31G unterstützt werdenWenn 802.11A, RM21A und RM22A unterstützt werdenDie Access Points der Serie 1200 können mit einer beliebigen Kombination von unterstützten Funkmodulen aufgerüstet werden: Nur G, nur A oder sowohl G als auch A. Wenn es sich bei einem Access Point mit zwei Funkmodulen um eine von LWAPP unterstützte Funkeinheit handelt, führt das Upgrade-Tool das Upgrade noch durch. Das Tool fügt dem detaillierten Protokoll eine Warnmeldung hinzu, die angibt, welche Funkübertragung nicht unterstützt wird.
- Alle Access Points der Serie 1310 AG
- Cisco C3201 Wireless Mobile Interface Card (WMIC)**Hinweis:** Die 802.11a-Funkmodule der zweiten Generation enthalten zwei Teilenummern.

Access Points müssen Cisco IOS Release 12.3(7)JA oder höher ausführen, bevor Sie das Upgrade durchführen können.

Für die Cisco C3201WMIC müssen die Access Points die Cisco IOS-Version 12.3(8)JK oder höher ausführen, bevor Sie das Upgrade durchführen können.

Diese Cisco Wireless LAN Controller unterstützen autonome Access Points, die auf den Lightweight-Modus aktualisiert wurden:

- Controller der Serie 2000
- Controller der Serie 2100
- Controller der Serie 4400
- Cisco Wireless Services Module (WiSMs) für Cisco Catalyst Switches der Serie 6500
- Controller-Netzwerkmodule der Cisco Integrated Services Router der Serien 28/37/38xx
- Catalyst 3750G Integrated Wireless LAN Controller Switches

Cisco Controller müssen mindestens Softwareversion 3.1 ausführen.

Das Cisco Wireless Control System (WCS) muss mindestens Version 3.1 ausführen. Das Aktualisierungsprogramm wird auf den Plattformen Windows 2000 und Windows XP unterstützt.

Sie können die neueste Version des Upgrade-Dienstprogramms von der Seite Cisco Software Downloads herunterladen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Upgrade-Prozess - Übersicht

Der Benutzer führt ein Upgrade-Dienstprogramm aus, das eine Eingabedatei mit einer Liste von Access Points und ihren Anmeldeinformationen akzeptiert. Das Dienstprogramm telnet den Access Points in der Eingabedatei eine Reihe von Cisco IOS-Befehlen zu, um den Access Point für das Upgrade vorzubereiten. Dazu gehören die Befehle zum Erstellen der selbstsignierten Zertifikate. Außerdem werden die Geräte mithilfe von Telnet-Verbindungen mit dem Controller programmiert, um die Autorisierung bestimmter selbstsignierter Access Points für Zertifikate zu ermöglichen. Anschließend wird die Cisco IOS Software Release 12.3(11)JX1 auf den Access Point geladen, damit er dem Controller beitreten kann. Wenn der Access Point dem Controller beitritt, lädt er eine vollständige Cisco IOS-Version von diesem herunter. Das Aktualisierungsprogramm generiert eine Ausgabedatei, die die Liste der Access Points und die entsprechenden selbstsignierten Schlüssel-Hash-Werte für Zertifikate enthält, die in die WCS-Verwaltungssoftware importiert werden können. Das WCS kann diese Informationen dann an andere Controller im Netzwerk senden.

Weitere Informationen finden Sie im Abschnitt zum Upgrade-Verfahren für das Upgrade autonomer Cisco Aironet Access Points auf den Lightweight-Modus.

Upgrade-Tool - Grundlegender Betrieb

Dieses Aktualisierungstool wird verwendet, um einen autonomen Access Point auf den Lightweight-Modus zu aktualisieren, sofern der Access Point für dieses Upgrade kompatibel ist. Das Upgrade-Tool führt die grundlegenden Aufgaben aus, die für ein Upgrade vom autonomen auf den Lightweight-Modus erforderlich sind. Zu diesen Aufgaben gehören:

- Grundlegende Statusprüfung - Überprüft, ob der Access Point unterstützt wird, ob eine minimale Softwareversion ausgeführt wird und ob die Funktypen unterstützt werden.
- Stellen Sie sicher, dass der Access Point als Root konfiguriert ist.
- Vorbereitung des autonomen Access Points zur Konvertierung: Fügt die PKI-Konfigurations- und Zertifikathierarchie (Public Key Infrastructure) hinzu, sodass die AP-Authentifizierung für die Cisco Controller erfolgen kann, und für den Access Point können selbst signierte Zertifikate (SSCs) generiert werden. Wenn der Access Point über ein in der Fertigung installiertes Zertifikat (MIC) verfügt, werden keine SSCs verwendet.
- Lädt ein Autonomous-to-Lightweight Mode-Upgrade-Image herunter, z. B. 12.3(11)JX1 oder 12.3(7)JX, mit dem der Access Point einem Controller beitreten kann. Nach erfolgreichem Download wird der Access Point neu gestartet.
- Generiert eine Ausgabedatei, die aus AP-MAC-Adressen, dem Zertifikatstyp und einem sicheren Schlüssel-Hash besteht, und aktualisiert den Controller automatisch. Die Ausgabedatei kann in WCS importiert und an andere Controller exportiert werden.

Wichtige Hinweise

Bevor Sie dieses Dienstprogramm verwenden, bedenken Sie die folgenden wichtigen Hinweise:

- Access Points, die mit diesem Tool konvertiert wurden, sind nicht mit den Controllern 40xx, 41xx oder 3500 verbunden.
- Access Points können nicht mit 802.11b-Funkmodulen oder 802.11a-Funkmodulen der ersten Generation aktualisiert werden.
- Wenn Sie die statische IP-Adresse, Netzmaske, den Hostnamen und das Standard-Gateway der Access Points nach der Konvertierung und dem Neustart beibehalten möchten, müssen Sie eines dieser autonomen Bilder auf die Access Points laden, bevor Sie die Access Points auf LWAPP verdecken:12,3(7)JA12.3(7)JA112.3(7)JA212,3(7)JA312.3(7)JA412,3(8)JA12.3(8)JA112.3(8)JA212.3(8)JEA12,3(8)JEA112.3(8)JEA212.3(8)JEB12.3(8)JEB112,4(3 g) JA12,4(3 g) JA1
- Wenn Sie Access Points von einem dieser autonomen Images auf LWAPP aktualisieren, behalten die konvertierten Access Points ihre statische IP-Adresse, Netzmaske, den Hostnamen und das Standard-Gateway nicht bei:12,3(11)JA12.3(11)JA112.3(11)JA212,3(11)JA3
- Das LWAPP-Aktualisierungstool gibt Windows-Speicherressourcen nicht frei, wenn der Aktualisierungsvorgang abgeschlossen ist. Speicherressourcen werden erst freigegeben, nachdem Sie das Aktualisierungstool beendet haben. Wenn Sie mehrere Batches von Access Points aktualisieren, müssen Sie das Tool zwischen den Stapeln beenden, um Speicherressourcen freizugeben. Wenn Sie das Programm nicht zwischen den Stapeln beenden, nimmt die Leistung der Upgrade-Station aufgrund des übermäßigen Speicherverbrauchs schnell ab.

Arten von Zertifikaten

Es gibt zwei verschiedene Arten von APs:

- APs mit einem MIC
- APs, die SSC benötigen

Auf werkseitig installierte Zertifikate wird der Begriff "MIC" verwiesen, der ein Akronym für das von der Fertigung installierte Zertifikat ist. Cisco Aironet Access Points, die vor dem 18. Juli 2005 ausgeliefert wurden, verfügen über kein MIC. Daher erstellen diese Access Points bei einem Upgrade auf den Lightweight-Modus ein selbstsigniertes Zertifikat. Controller sind so programmiert, dass sie selbstsignierte Zertifikate für die Authentifizierung bestimmter Access Points akzeptieren.

Sie müssen Cisco Aironet MIC APs, die LWAPP (Lightweight Access Point Protocol) verwenden, wie Aironet 1000 APs, behandeln und eine entsprechende Fehlerbehebung durchführen. Mit anderen Worten: Überprüfen Sie die IP-Verbindung, debuggen Sie den LWAPP-Statuscomputer, und überprüfen Sie dann die Verschlüsselung.

Die Upgrade-Tool-Protokolle zeigen an, ob es sich bei dem Access Point um einen MIC AP oder einen SSC-AP handelt. Dies ist ein Beispiel für ein detailliertes Protokoll vom Aktualisierungstool:

```
2006/08/21 16:59:07 INFO  172.16.1.60  Term Length configured.
```

```
2006/08/21 16:59:07 INFO  172.16.1.60  Upgrade Tool supported AP
2006/08/21 16:59:07 INFO  172.16.1.60  AP has two radios
2006/08/21 16:59:07 INFO  172.16.1.60  AP has Supported Radio
2006/08/21 16:59:07 INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO  172.16.1.60  Station role is  Root AP
2006/08/21 16:59:07 INFO  172.16.1.60  MIC is already configured in the AP
2006/08/21 16:59:07 INFO  172.16.1.60      Hardware is PowerPC405GP Ethernet,
                                         address is 0015.63e5.0c7e (bia 0015.63e5.0c7e)
2006/08/21 16:59:08 INFO  172.16.1.60  Inside Shutdown function
2006/08/21 16:59:10 INFO  172.16.1.60  Shutdown the Dot11Radio1
2006/08/21 16:59:11 INFO  172.16.1.60  Shutdown the Dot11Radio0
2006/08/21 16:59:12 INFO  172.16.1.60  Updating the AP with Current System Time
2006/08/21 16:59:13 INFO  172.16.1.60  Saving the configuration into memory
2006/08/21 16:59:13 INFO  172.16.1.60  Getting  AP Name
2006/08/21 16:59:58 INFO  172.16.1.60  Successfully Loaded the LWAPP Recovery
                                         Image on to the AP
2006/08/21 16:59:58 INFO  172.16.1.60  Executing Write Erase Command
2006/08/21 17:00:04 INFO  172.16.1.60  Flash contents are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Environmental Variables are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Reloading the AP
2006/08/21 17:00:08 INFO  172.16.1.60  Successfully executed the Reload command
```

In diesem Protokoll gibt die hervorgehobene Zeile an, dass im Access Point eine MIC installiert ist. Weitere Informationen zu den Zertifikaten und zum Upgrade-Prozess finden Sie im Abschnitt Upgrade Process Overview (Upgrade-Prozess-Übersicht) im Abschnitt Upgrade Autonomous Cisco Aironet Access Points to Lightweight Mode (Upgrade autonomer Cisco Aironet Access Points auf Lightweight-Modus).

Bei den SSC-APs wird auf dem Controller kein Zertifikat erstellt. Beim Aktualisierungstool generiert der AP ein Rivest-, Shamir- und Adelman-Schlüsselpaar (RSA), das zum Signieren eines selbst erstellten Zertifikats (SSC) verwendet wird. Das Upgrade-Tool fügt der Controller-Authentifizierungsliste einen Eintrag mit der MAC-Adresse des Access Points und dem öffentlichen Schlüssel-Hash hinzu. Der Controller benötigt den öffentlichen Schlüssel-Hash, um die SSC-Signatur zu validieren.

Wenn der Eintrag dem Controller nicht hinzugefügt wurde, überprüfen Sie die CSV-Ausgabedatei. Für jeden Access Point sollten Einträge vorhanden sein. Wenn Sie den Eintrag finden, importieren Sie diese Datei in den Controller. Wenn Sie die Befehlszeilenschnittstelle (CLI) des Controllers (mit dem Befehl **config auth-list**) oder das Switch-Web verwenden, müssen Sie jeweils eine Datei importieren. Mit einem WCS können Sie die gesamte CSV-Datei als Vorlage importieren.

Überprüfen Sie auch die Zulassung.

Hinweis: Wenn Sie über einen LAP-AP verfügen, aber Cisco IOS-Funktionen wünschen, müssen Sie ein autonomes Cisco IOS-Image darauf laden. Umgekehrt können Sie ein LWAPP-Wiederherstellungs-Image über autonomes IOS installieren, wenn Sie einen autonomen Access Point haben und ihn in LWAPP konvertieren möchten.

Sie können die Schritte zum Ändern des AP-Images mit der MODE-Schaltfläche oder den Befehlen **zum Herunterladen** des CLI-**Archivs** ausführen. Unter Problembehandlung finden Sie weitere Informationen zur Verwendung des MODE-Schaltflächen-Image-Neuladevorgangs, das mit autonomem IOS oder Wiederherstellungs-Image funktioniert, das als Standard-Dateiname des AP-Modells bezeichnet wird.

Im nächsten Abschnitt werden einige der häufig auftretenden Probleme bei der Aktualisierung sowie die Schritte zur Behebung dieser Probleme beschrieben.

Problem

Symptom

Der Access Point wird nicht zum Controller hinzugefügt. Im Abschnitt Solutions dieses Dokuments werden die Ursachen nach Wahrscheinlichkeit aufgeführt.

Lösungen

Verwenden Sie diesen Abschnitt, um dieses Problem zu beheben.

Ursache 1

Der Access Point kann den Controller nicht über die LWAPP-Erkennung finden, oder der Access Point kann den Controller nicht erreichen.

Fehlerbehebung

Führen Sie diese Schritte aus:

1. Geben Sie den Befehl **debug lwapp events enable** in der Controller-CLI aus.Suchen Sie nach der LWAPP Discovery Response > join request > join response sequenz. Wenn die LWAPP-Erkennungsanfrage nicht angezeigt wird, bedeutet dies, dass der Access Point den Controller nicht finden kann oder nicht findet.Im Folgenden finden Sie ein Beispiel für eine erfolgreiche JOIN-ANTWORT vom Wireless LAN Controller (WLC) auf den konvertierten Lightweight AP (LAP). Dies ist die Ausgabe des Befehls **debug lwapp events enable**:
```
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP
                          00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
                          00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
                          to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
                          00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
                          to ff:ff:ff:ff:ff:ff on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to
                          AP 00:15:63:e5:0c:7e on Port 1
Thu May 25 06:54:05 2006: Received LWAPP JOIN REQUEST from AP 00:15:63:e5:0c:7e
                          to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:54:05 2006: LWAPP Join-Request MTU path from AP 00:15:63:e5:0c:7e
                          is 1500, remote debug mode is 0
Thu May 25 06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e
                          (index 51)Switch IP: 172.16.1.11, Switch Port: 12223,
                          intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679,
                          next hop MAC: 00:15:63:e5:0c:7e
Thu May 25 06:54:05 2006: Successfully transmission of LWAPP Join-Reply to AP
                          00:15:63:e5:0c:7e
.......................................
.......................................
..................................... // the debug output continues for
full registration process.
```
2. Überprüfen Sie, ob IP-Verbindungen zwischen dem AP-Netzwerk und dem Controller

vorhanden sind. Wenn sich der Controller und der Access Point im gleichen Subnetz befinden, stellen Sie sicher, dass sie ordnungsgemäß miteinander verbunden sind. Wenn sie sich in unterschiedlichen Subnetzen befinden, stellen Sie sicher, dass zwischen ihnen ein Router verwendet wird und das Routing zwischen den beiden Subnetzen ordnungsgemäß aktiviert ist.

3. Überprüfen der ordnungsgemäßen Konfiguration des ErkennungsmechanismusWenn die DNS-Option (Domain Name System) zum Ermitteln des WLC verwendet wird, stellen Sie sicher, dass der DNS-Server korrekt konfiguriert ist, um die lokale Domäne CISCO-LWAPP-CONTROLLER.CISCO der WLC-IP-Adresse zuzuordnen. Wenn der Access Point den Namen auflösen kann, sendet er eine LWAPP-Join-Nachricht an die aufgelöste IP-Adresse.Wenn Option 43 als Erkennungsoption verwendet wird, stellen Sie sicher, dass diese auf dem DHCP-Server korrekt konfiguriert ist.Unter Registrieren der LAP beim WLC finden Sie weitere Informationen zum Erkennungsprozess und zur Sequenz.Weitere Informationen zur Konfiguration der DHCP-Option 43 finden Sie unter Konfigurationsbeispiel für die DHCP-OPTION 43 für Lightweight Cisco Aironet Access Points.**Hinweis:** Beachten Sie, dass bei der Konvertierung statisch adressierter APs der einzige funktionierende Layer-3-Erkennungsmechanismus der DNS ist, da die statische Adresse während des Upgrades erhalten bleibt.Auf dem Access Point können Sie den Befehl **debug lwapp client events** und den Befehl **debug ip udp** ausführen, um genügend Informationen zu erhalten, um genau zu bestimmen, was geschieht. Es sollte eine UDP-Paketsequenz (User Datagram Protocol) wie die folgende angezeigt werden:Von der AP-IP mit der Controller-Verwaltungsschnittstelle IP bezogen.Von der IP-Adresse des Controller-AP-Managers an die AP-IP-Adresse übertragen.Paketserie, die von der AP-IP zur AP-Manager-IP-Adresse stammt.**Hinweis:** In einigen Situationen kann es mehrere Controller geben, und der Access Point kann versuchen, einem anderen Controller auf der Grundlage des LWAPP-Discovery State-Systems und der Algorithmen beizutreten. Diese Situation kann aufgrund des standardmäßigen dynamischen AP-Lastenausgleichs auftreten, den der Controller ausführt. Diese Situation kann eine Prüfung verdienen.**Hinweis:** Dies ist eine Beispielausgabe des Befehls **debug ip udp**:

```
Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12222),
                     length=78
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=60
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223),
                     length=75
*Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679),
                     length=59
*Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=180
*Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=89
*Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=209
*Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=164
*Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
```

```
                        length=22
*Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                        length=209
*Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                        length=22
*Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                        length=287
*Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                        length=22
*Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                        length=89
*Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                        length=22
*Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                        length=222
```

Auflösung

Führen Sie diese Schritte aus:

1. Lesen Sie das Handbuch.
2. Korrigieren Sie die Infrastruktur, sodass sie die LWAPP-Erkennung korrekt unterstützt.
3. Setzen Sie den Access Point in das gleiche Subnetz wie den Controller, um ihn zu entlasten.
4. Führen Sie ggf. den Befehl **lwapp controller ip address *A.B.C.D* aus**, um die Controller-IP in der AP-CLI manuell festzulegen:Der *A.B.C.D*-Teil dieses Befehls ist die IP-Adresse der Verwaltungsschnittstelle des WLC.**Hinweis:** Dieser CLI-Befehl kann für einen Access Point verwendet werden, der noch nie für einen Controller registriert wurde, oder für einen Access Point, dessen Standard-Aktivierungskennwort geändert wurde, während er mit einem vorherigen Controller verbunden ist. Weitere Informationen finden Sie unter Zurücksetzen der LWAPP-Konfiguration auf einem Lightweight AP (LAP).

Ursache 2

Die Controller-Zeit liegt außerhalb des Zertifikatsvalidierungsintervalls.

Fehlerbehebung

Führen Sie diese Schritte aus:

1. Geben Sie die **Debug-App-Fehler enable enable** und **debug pm pki enable-**Befehle ein.Diese **Debugbefehle** zeigen das Debuggen von Zertifikatsmeldungen an, die zwischen dem Access Point und dem WLC übergeben werden. Die Befehle zeigen eindeutig an, dass das Zertifikat als außerhalb des Gültigkeitsintervalls abgelehnt wird.**Hinweis:** Achten Sie darauf, den UTC-Offset (Coordinated Universal Time) zu berücksichtigen.Dies ist die Ausgabe des Befehls **debug pm pki enable** auf dem Controller:
```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
                          L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
                          MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
                          CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
```

```
                          00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
.........................
.........................
.........................
.........................
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
                          >cscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
                          2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
                          validity interval: make sure the controller time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

Beachten Sie in dieser Ausgabe die hervorgehobenen Informationen. Diese Informationen zeigen deutlich, dass die **Controller-Zeit außerhalb des Zertifikatsvalidierungsintervalls des Access Points liegt**. Aus diesem Grund kann sich der Access Point nicht beim Controller registrieren. Zertifikate, die im AP installiert sind, haben ein vordefiniertes Gültigkeitsintervall. Die Zeit für den Controller sollte so festgelegt werden, dass sie innerhalb des Zertifikatsvalidierungsintervalls des Access Points liegt.

2. Geben Sie den Befehl **show crypto ca certificate** aus der AP-CLI aus, um das im Access Point festgelegte Gültigkeitsintervall für Zertifikate zu überprüfen.Dies ist ein Beispiel:

```
AP0015.63e5.0c7e#show crypto ca certificates
.........................................
.........................................
.........................................
.............................................
Certificate
  Status: Available
  Certificate Serial Number: 4BC6DAB80000000517AF
  Certificate Usage: General Purpose
  Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
  Subject:
    Name: C1200-001563e50c7e
    ea=support@cisco.com
    cn=C1200-001563e50c7e
    o=Cisco Systems
    l=San Jose
    st=California
    c=US
  CRL Distribution Point:
    http://www.cisco.com/security/pki/crl/cmca.crl
  Validity Date:
    start date: 17:22:04 UTC Nov 30 2005
    end   date: 17:32:04 UTC Nov 30 2015
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: Cisco_IOS_MIC_cert
.................................
.................................
.................................
```

Die gesamte Ausgabe wird nicht aufgelistet, da mit der Ausgabe dieses Befehls viele Gültigkeitsintervalle verbunden sein können. Sie müssen nur das vom **Associated Trustpoint** angegebene Gültigkeitsintervall berücksichtigen**: Cisco_IOS_MIC_cert** mit dem entsprechenden AP-Namen im Namensfeld (**Hier, Name: C1200-001563e50c7e**), wie in diesem Ausgabebeispiel hervorgehoben. **Dies ist das tatsächliche Gültigkeitsintervall für Zertifikate, das berücksichtigt werden muss.**

3. Führen Sie den Befehl **show time** aus der Controller-CLI aus, um zu überprüfen, ob das auf

dem Controller festgelegte Datum und die Uhrzeit unter dieses Gültigkeitsintervall fallen.Wenn die Controller-Zeit über oder unter diesem Gültigkeitsintervall für Zertifikate liegt, ändern Sie die Controller-Zeit so, dass sie in dieses Intervall fällt.

Auflösung

Führen Sie diesen Schritt aus:

Wählen Sie **Befehle > Uhrzeit** im GUI-Modus des Controllers aus, oder geben Sie den Befehl **config time** in der Controller-CLI aus, um die Controller-Zeit festzulegen.

Ursache 3

Bei SSC-APs ist die SSC-AP-Richtlinie deaktiviert.

Fehlerbehebung

In solchen Fällen wird diese Fehlermeldung auf dem Controller angezeigt:

```
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest
                          :spamDecodeJoinReq failed
Wed Aug  9 17:20:21 2006  [ERROR] spam_crypto.c 1509: Unable to free public key for
                          AP 00:12:44:B3:E5:60
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include
                          valid certificate in CERTIFICATE_PAYLOAD from
                          AP 00:12:44:b3:e5:60.
Wed Aug  9 17:20:21 2006  [CRITICAL] sshpmPkiApi.c 1493: Not configured to accept
                          Self-signed AP cert
```

Führen Sie diese Schritte aus:

Führen Sie eine der folgenden beiden Aktionen aus:

- Führen Sie den Befehl **show auth-list** in der Controller-CLI aus, um zu überprüfen, ob der Controller für die Annahme von APs mit SSCs konfiguriert ist.Dies ist eine Beispielausgabe des Befehls **show auth-list**:

```
#show auth-list

Authorize APs against AAA ..... disabled

Allow APs with Self-signed Certificate (SSC) .... enabled

Mac Addr                  Cert Type    Key Hash

----------------------    ----------   ----------------------------------------

00:09:12:2a:2b:2c         SSC          1234567890123456789012345678901234567890
```

- Wählen Sie **Security > AP Policies (Sicherheit > AP-Richtlinien)** in der GUI aus.

1. Überprüfen Sie, ob das Kontrollkästchen **Selbstsigniertes Zertifikat akzeptieren** aktiviert ist.

Ist dies nicht der Fall, aktivieren Sie es.
2. Wählen Sie **SSC** als Zertifikatstyp aus.
3. Fügen Sie **AP** zur Autorisierungsliste mit MAC-Adresse und Schlüssel-Hash hinzu.Dieser Schlüssel-Hash kann aus der Ausgabe des Befehls **debug pm pki enable** abgerufen werden. Weitere Informationen zum Abrufen des Schlüssel-Hash-Werts finden Sie Ursache 4.

Ursache 4

Der öffentliche SSC-Schlüssel-Hash ist falsch oder fehlt.

Fehlerbehebung

Führen Sie diese Schritte aus:

1. Geben Sie den Befehl **debug lwapp events enable ein**.Stellen Sie sicher, dass der Access Point beitreten möchte.
2. Geben Sie den Befehl **show auth-list** ein.Dieser Befehl zeigt den öffentlichen Schlüssel-Hash an, den der Controller im Speicher hat.
3. Geben Sie den Befehl **debug pm pki enable ein**.Dieser Befehl zeigt den tatsächlichen öffentlichen Schlüssel-Hash an. Der tatsächliche öffentliche Schlüssel-Hash muss mit dem öffentlichen Schlüssel-Hash übereinstimmen, den der Controller im Speicher hat. Eine Diskrepanz verursacht das Problem. Dies ist eine Beispielausgabe dieser Debugmeldung:

```
(Cisco Controller) > debug pm pki enable

Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle...
Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert>
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
>bsnDefaultRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscoDefaultMfgCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert<
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
Data
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  30820122 300d0609
2a864886 f70d0101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  01050003 82010f00
3082010a 02820101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  00c805cd 7d406ea0
cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  82fc0df0 39f2bff7
ad425fa7 face8f15
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f356a6b3 9b876251
43b95a34 49292e11
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  038181eb 058c782e
56f0ad91 2d61a389
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f81fa6ce cd1f400b
b5cf7cef 06ba4375
```

```
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  dde0648e c4d63259
774ce74e 9e2fde19
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  0f463f9e c77b79ea
65d8639b d63aa0e3
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  7dd485db 251e2e07
9cd31041 b0734a55
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  463fbacc 1a61502d
c54e75f2 6d28fc6b
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  82315490 881e3e31
02d37140 7c9c865a
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  9ef3311b d514795f
7a9bac00 d13ff85f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  97e1a693 f9f6c5cb
88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  ca364f6f 76cf78bc
bc1acc13 0d334aa6
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  031fb2a3 b5e572df
2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  fe64641f de2a6fe3
23311756 8302b8b8
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  1bfae1a8 eb076940
280cbed1 49b2d50f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  f7020301 0001
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This is the actual SSC key-hash value. Mon May 22 06:34:14 2006: LWAPP Join-Request
MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14
2006: spamRadiusProcessResponse: AP Authorization failure for
00:0e:84:32:04:f0
```

Auflösung

Führen Sie diese Schritte aus:

1. Kopieren Sie den öffentlichen Schlüssel-Hash aus der **debug pm pki enable-**Befehlsausgabe, und ersetzen Sie damit den öffentlichen Schlüssel-Hash in der Authentifizierungsliste.
2. Geben Sie den Befehl **config auth-list add ssc *AP_MAC AP_key* ein, um die MAC-Adresse und den Schlüssel-Hash zur Autorisierungsliste hinzuzufügen:**Dies ist ein Beispiel für diesen Befehl:

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

Ursache 5

Der Access Point weist ein Zertifikat oder einen öffentlichen Schlüssel auf.

Fehlerbehebung

Führen Sie diesen Schritt aus:

Geben Sie die **Debug-App-Fehler enable enable** und **debug pm pki enable-**Befehle ein.

Sie sehen Meldungen, die die beschädigten Zertifikate oder Schlüssel angeben.

Auflösung

Verwenden Sie eine der folgenden beiden Optionen, um das Problem zu beheben:

- MIC AP - Fordern Sie eine Retourengenehmigung (Return Materials Authorization, RMA) an.
- SSC AP - Downgrade auf Cisco IOS Software Release 12.3(7)JA.Gehen Sie wie folgt vor, um ein Downgrade durchzuführen:

1. Verwenden Sie die Option Reset Button (Reset-Taste).
2. Löschen Sie die Controller-Einstellungen.
3. Führen Sie das Upgrade erneut aus.

Ursache 6

Der Controller funktioniert möglicherweise im Layer-2-Modus.

Fehlerbehebung

Führen Sie diesen Schritt aus:

Überprüfen Sie den Betriebsmodus des Controllers.

Konvertierte APs unterstützen nur die Layer-3-Erkennung. Konvertierte APs unterstützen keine Layer-2-Erkennung.

Auflösung

Führen Sie diese Schritte aus:

1. Legen Sie fest, dass sich der WLC im Layer-3-Modus befindet.
2. Starten Sie neu, und geben Sie der AP-Manager-Schnittstelle eine IP-Adresse im gleichen Subnetz wie der Verwaltungsschnittstelle an.Wenn Sie einen Service-Port haben, z. B. den Service-Port eines 4402 oder 4404, sollten Sie ihn in einem anderen Supernet als den AP-Manager und die Verwaltungsschnittstellen haben.

Ursache 7

Dieser Fehler wird während der Aktualisierung angezeigt:

```
FAILED   Unable to Load  the LWAPP Recovery Image on to the AP
```

Fehlerbehebung

Gehen Sie wie folgt vor, wenn Sie diesen Fehler sehen:

1. Überprüfen Sie, ob Ihr TFTP-Server ordnungsgemäß konfiguriert ist.Wenn Sie den integrierten TFTP-Server des Upgrade-Tools verwenden, ist eine häufige Sorge die persönliche Firewall-Software, die das eingehende TFTP blockiert.
2. Überprüfen Sie, ob Sie das richtige Image für das Upgrade verwenden.Das Upgrade auf den

Lightweight-Modus erfordert ein spezielles Image und funktioniert nicht mit den normalen Upgrade-Images.

Ursache 8

Sie erhalten diese Fehlermeldung auf dem Access Point nach der Konvertierung:

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_
                     certs no certs in the SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
                     Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

Der Access Point wird nach 30 Sekunden neu geladen und startet den Vorgang erneut.

Auflösung

Führen Sie diesen Schritt aus:

Sie haben einen SSC-AP. Wenn Sie in den LWAPP AP konvertiert haben, fügen Sie den SSC und seine MAC-Adresse unter der AP-Authentifizierungsliste im Controller hinzu.

Tipps zur Fehlerbehebung

Diese Tipps können verwendet werden, wenn Sie vom autonomen zum LWAPP-Modus wechseln:

- Wenn der NVRAM nicht gelöscht wird, wenn der Controller versucht, nach der Konvertierung darauf zu schreiben, werden Probleme verursacht. Cisco empfiehlt, die Konfiguration zu löschen, bevor Sie einen Access Point in LWAPP umwandeln. So löschen Sie die Konfiguration:Gehen Sie in der IOS-GUI zu **Systemsoftware > Systemkonfiguration > Auf Standardeinstellungen zurücksetzen**, oder **Zurücksetzen auf Standardwerte mit Ausnahme von IP**.From CLI (Von CLI ausführen) - Geben Sie die Befehle **zum Löschen** und **erneuten Laden** der **Schreibvorgänge** über die CLI aus, und lassen Sie die Konfiguration nicht zu, wenn Sie dazu aufgefordert werden.Dadurch wird auch die Erstellung der Textdatei der APs, die mit dem Upgrade-Tool konvertiert werden sollen, einfacher, da die Einträge zu <ip address>,Cisco,Cisco,Cisco werden.
- Cisco empfiehlt die Verwendung von tftp32. Sie können den neuesten TFTPD-Server unter http://tftpd32.jounin.net/ herunterladen.
- Wenn während des Aktualisierungsvorgangs eine Firewall oder eine Zugriffskontrollliste aktiviert ist, kann das Upgrade-Tool die Datei, die Umgebungsvariablen enthält, nicht von einer Workstation auf einen Access Point kopieren.Wenn eine Firewall oder eine Zugriffskontrollliste den Kopiervorgang blockiert und Sie die Option "Use Upgrade Tool TFTP Server" (Upgrade-Tool für TFTP-Server verwenden) auswählen, können Sie mit dem Upgrade nicht fortfahren, da das Tool die Umgebungsvariablen nicht aktualisieren kann und der Image-Upload zum AP fehlschlägt.
- Überprüfen Sie das Image, auf das Sie aktualisieren möchten. Das Upgrade von IOS auf LWAPP-Images unterscheidet sich von den normalen IOS-Images.Deaktivieren Sie unter

Eigene Dateien/Arbeitsplatz—> Tools—> Ordneroptionen das Kontrollkästchen **Dateierweiterungen für bekannte Dateitypen ausblenden**.

- Verwenden Sie immer das neueste verfügbare Upgrade-Tool und das Upgrade Recovery Image. Die neuesten Versionen sind im Wireless Software Center verfügbar.
- Ein Access Point kann eine **.tar-**Image-Datei nicht booten. Es ist ein Archiv, ähnlich wie ZIP-Dateien. Sie müssen die **.tar**-Datei mit dem Befehl **Archive download** in den AP-Flash entpacken oder das bootfähige Image zuerst aus der TAR-Datei ziehen und dann das bootfähige Image in den AP-Flash-Speicher legen.

Zugehörige Informationen

- Upgrade autonomer Cisco Aironet Access Points auf Lightweight-Modus
- Zurücksetzen der LWAPP-Konfiguration auf einem Lightweight AP (LAP)
- Konfigurationsbeispiel für DHCP OPTION 43 für Lightweight Cisco Aironet Access Points
- Wiederherstellen des Hashschlüssels des Access Points und Importieren des Hashschlüssels in den Controller
- Kann der Cisco Aironet Autonomous Access Point mithilfe der CLI in LWAPP (Lightweight Access Point Protocol) umgewandelt werden?
- Technischer Support und Dokumentation für Cisco Systeme