ハイ アベイラビリティ(SSO)導入ガイド

最終更新日:2018 年 3 月 28 日

はじめに

このガイドでは、アクセス ポイントおよびクライアントのステートフル スイッチオーバー(AP およびクライアント SSO)のサポートに関連する Cisco Unified Wireless LAN Controller(WLC)の操作と設定のセオリーについて説明します。

Cisco Unified Wireless Network ソフトウェア リリース バージョン 8.0 およびそれ以降の新しいハイ アベイラビリティ(HA)機能セットである AP SSO を使用すると、アクセス ポイント(AP)でアクティブ WLC との CAPWAP トンネルを確立でき、AP データベースのミラー コピーをスタンバイ WLC と共有できます。アクティブ WLC が故障した場合、AP は Discovery 状態にならず、スタンバイ WLC がアクティブ WLC としてネットワークを引き継ぎます。

任意の時点で、AP とアクティブ状態の WLC の間で維持される CAPWAP トンネルは 1 つだけです。Cisco Unified Wireless LAN に AP SSO サポートが追加されたのは、障害状態によって引き起こされるワイヤレス ネットワークの大規模なダウンタイムを削減することを全体的な目標としています。この障害状態は、ボックス フェールオーバーまたはネットワーク フェールオーバーが原因で発生する可能性があります。

サービスに影響を与えずにハイ アベイラビリティをサポートするには、アクティブ コントローラからスタンバイ コントローラへのクライアントおよび AP のシームレスな遷移をサポートすることが必要となります。リリース 7.5 では、クライアント ステートフル スイッチ オーバー(クライアント SSO)をワイヤレス LAN コントローラでサポートしています。クライアント SSO がサポートされるのは、すでに認証および DHCP フェーズが完了し、トラフィックを通しはじめたクライアントです。SSO クライアントによって、WLC にクライアントが関連付けられたときまたはクライアントのパラメータが変更されたときに、クライアント情報はスタンバイ WLC へ同期します。完全に認証済みのクライアント(Run 状態のクライアントなど)はスタンバイへと同期され、スイッチオーバー時のクライアントの再関連付けは回避されます。これによりクライアントと AP のフェールオーバーはシームレスになり、クライアント サービスのダウンタイム ゼロと SSID の非停止が実現します。

WLC およびリリース 8.7 でサポートされている AP

このマニュアルの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- WLC 3500 シリーズ、8500 シリーズ、および 5520
- レガシーの Wave-1 AP:3700、2700、1700、702、702W、1530、1570
- Wave-2 AP:1800 シリーズ、2800 シリーズ、3800 シリーズ、1540、1560
- このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定(デフォルト)の状態から作業が開始されています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

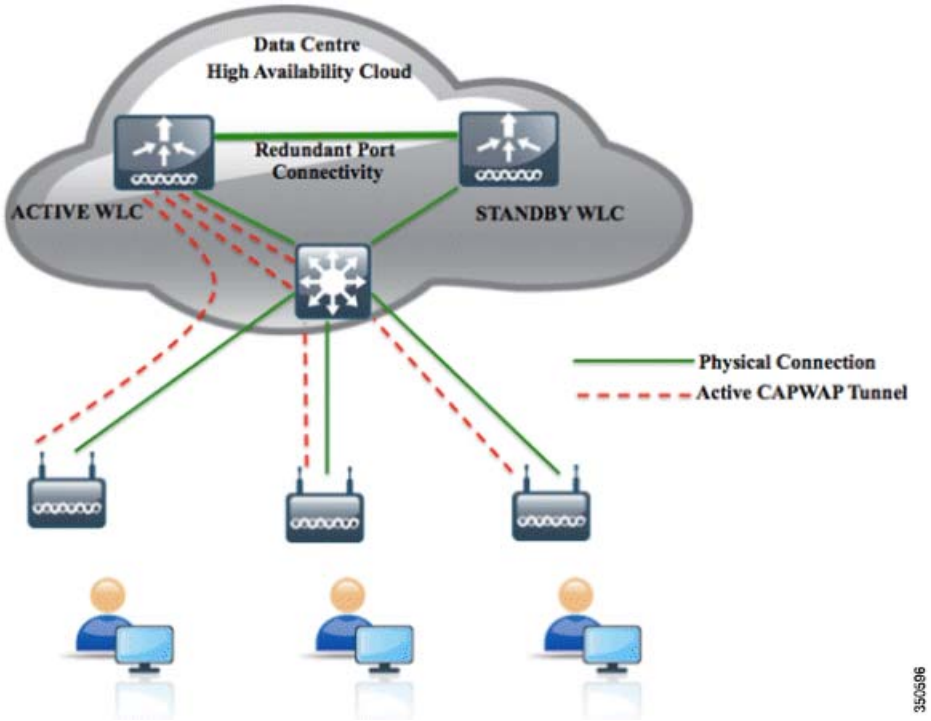
注:5508、7500、8510 および WiSM-2 は、リリース 8.5 までサポートされています。3504 シリーズはリリース 8.5 からサポートされています。詳細については、リリース ノートを参照してください。

表記法

ドキュメント表記の詳細は、『Cisco Technical Tips Conventions』を参照してください。

トポロジ

このドキュメントでは、次のネットワーク トポロジを使用しています。



製品や機能の概要

HA の新しいアーキテクチャは、ボックスツーボックス冗長性を目的としています。つまり、1 つの WLC がアクティブ状態になり、2 つ目の WLC が冗長ポートを介してアクティブ WLC の状態を継続的にモニタするホット スタンバイ状態になる 1 対 1 対応です。両方の WLC では、管理インターフェイスの IP アドレスなど、同じ設定を共有します。設定全体が冗長ポートを介してアクティブ WLC からスタンバイ WLC に同期されるため(起動時のバルク設定および実行時の増分設定)、スタンバイ状態の WLC を個別に設定する必要はありません。AP の CAPWAP 状態(run 状態の AP のみ)も同期され、AP データベースのミラー コピーがスタンバイ WLC 上で維持されます。アクティブ WLC が故障した場合、AP は Discovery 状態にならず、スタンバイ WLC がネットワークのアクティブ WLC を引き継ぎます。プリエンプション機能はありません。以前のアクティブ WLC が復帰した場合、この WLC はアクティブ WLC の役割を引き継ぎませんが、現在のアクティブ WLC と状態をネゴシエートしてスタンバイ状態に遷移します。アクティブとスタンバイを決めるのは自動選択処理ではありません。アクティブとスタンバイの WLC は、リリース 7.3 以降では、HA SKU(製造時に注文される UDI)に基づいて決まります。HA SKU UDI を備えた WLC は、ブート時に、まずスタンバイ WLC になり、永久カウント ライセンスを実行している WLC とペアになります。永久カウント ライセンスのある既存の WLC の場合は、手動設定に基づいてアクティブとスタンバイが決定されます。

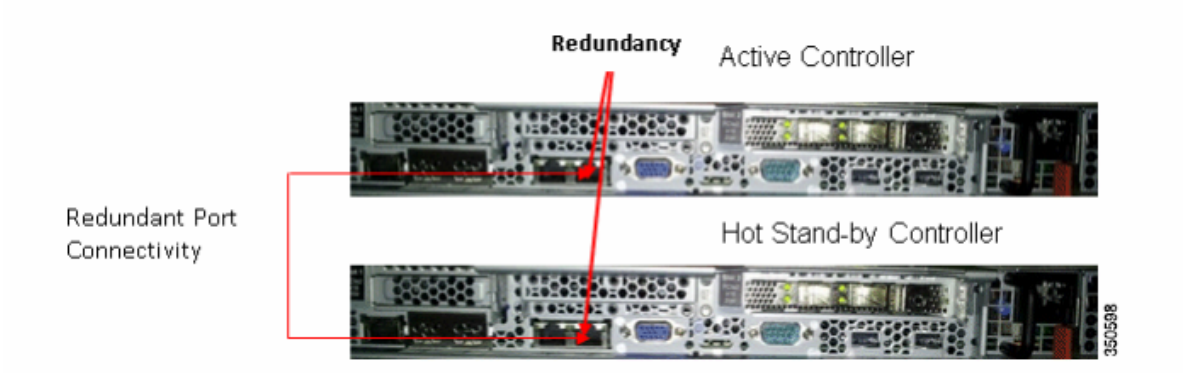
AP SSO は、5500/7500/8500 および WiSM-2 WLC でサポートされています。リリース 7.3 では、スイッチオーバー後に AP セッションが損なわれないことを保障する AP SSO のみをサポートしています。

クライアント SSO は 5500/7500/8500 および WiSM2 WLC でサポートされます(リリース 7.5 以降)。詳細については、「リリース 7.5 のハイ アベイラビリティ」(41 ページ)を参照してください。

クライアント SSO は 5520/3500/8500 WLC でサポートされます(リリース 8.5 以降)。

3504/5520/8500 での冗長ポートを使用した HA 接続

3500/5520/8500 WLC には、アクティブからスタンバイ WLC に設定を同期するためにバックツーバック接続する必要のある専用冗長ポートが装備されています。



5520 および 8540 と同様に、3504 ワイヤレス コントローラにもユニットの前面に冗長ポートがあります。他の WLC と同様、WLC 3504 も AP SSO とクライアント SSO の両方をサポートしています。以下に示すのは、HA セットアップで RP ポートを使用して 2 つの WLC 3504 に接続する方法(バックツーバック)です。

アクティブ WLC の状態を確認するために、冗長ポートを介してスタンバイからアクティブ WLC に 100 ミリ秒(デフォルト タイマー)ごとにキープアライブ パケットが送信されます。

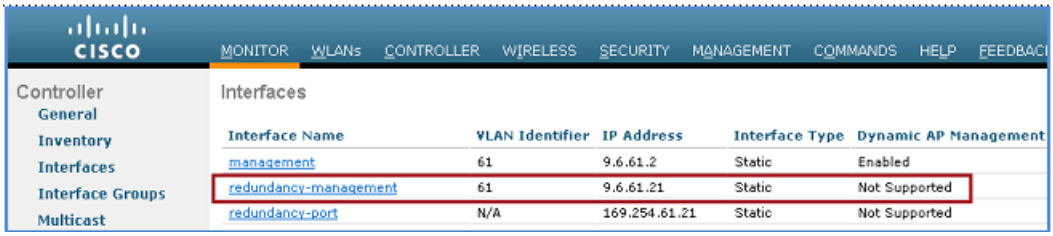
HA セットアップの両方の WLC がゲートウェイの到達可能性を追跡します。アクティブ WLC は、管理 IP アドレスを発信元に使用してインターネット制御メッセージ プロトコル(ICMP)の ping をゲートウェイに送信し、スタンバイ WLC は、冗長性管理 IP アドレスを使用して ICMP の ping をゲートウェイ送信します。両方の WLC が、1 秒間隔でゲートウェイに ICMP ping を送信します。冗長ポート間のバックツーバック直接接続を設けることを強くお勧めします。

注:アクティブとスタンバイの冗長ポート間を物理的に直接接続することを強くお勧めします。接続間の距離は、イーサネット ケーブルの規格によって 100 メートルまで可能です。

HA 連携のための新規インターフェイスの概要

冗長性管理インターフェイス

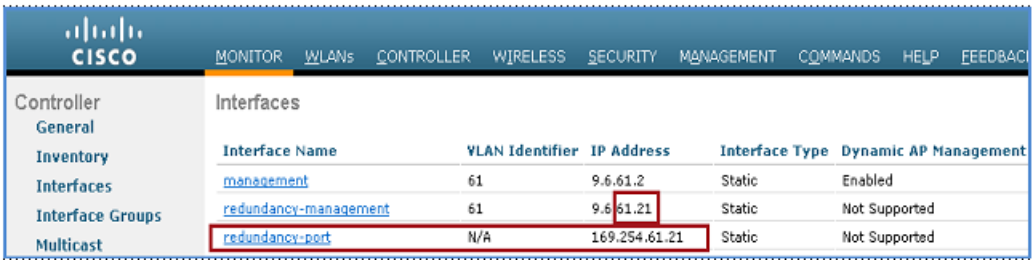
このインターフェイスには、管理インターフェイスと同じサブネットの IP アドレスを設定する必要があります。アクティブ WLC が冗長ポートのキープアライブ メッセージに応答しない場合は、このインターフェイスにより、ネットワーク インフラストラクチャを介してアクティブ WLC の状態が確認されます。これは、ネットワークとアクティブ WLC の追加のヘルス チェックになり、スイッチオーバーを実行する必要があるのかどうかの確認になります。スタンバイ WLC では、ゲートウェイの到達可能性を確認する ICMP ping パケットを発信する際も、このインターフェイスを使用します。このインターフェイスは、ボックス障害または手動リセットの際に、アクティブ WLC からスタンバイ WLC に通知を送信するためにも使用されます。スタンバイ WLC では、Syslog や NTP サーバ、およびすべての設定アップロードで TFTP サーバと通信するために、このインターフェイスを使用します。



冗長ポート

このインターフェイスは、新しい HA アーキテクチャで非常に重要な役割を持ちます。起動時のバルク設定と増分設定は、冗長ポートを使用してアクティブ WLC からスタンバイ WLC に同期されます。HA セットアップの WLC では、このポートを使用して HA 役割のネゴシエーションを実行します。冗長ポートは、100 ミリ秒(デフォルト タイマー)ごとにスタンバイ WLC からアクティブ WLC に UDP キープアライブ メッセージを送信してピアの到達可能性を確認するためにも使用されます。ボックス障害の際には、冗長ポートを介して、アクティブ WLC からスタンバイ WLC に対する通知も送信されます。NTP サーバが設定されていない場合は、冗長ポートを介して、アクティブ WLC からスタンバイ WLC への手動時刻同期が実行されます。スタンドアロン コントローラの場合のこのポートは、最後の 2 オクテットを冗長性管理インターフェイスの最後の 2 オクテットから取得して自動生成される IP アドレスが割り当てられます(先頭の 2 オクテットは常に 169.254)。

注:冗長性管理インターフェイスをタグなしのインターフェイスにすることはできません。

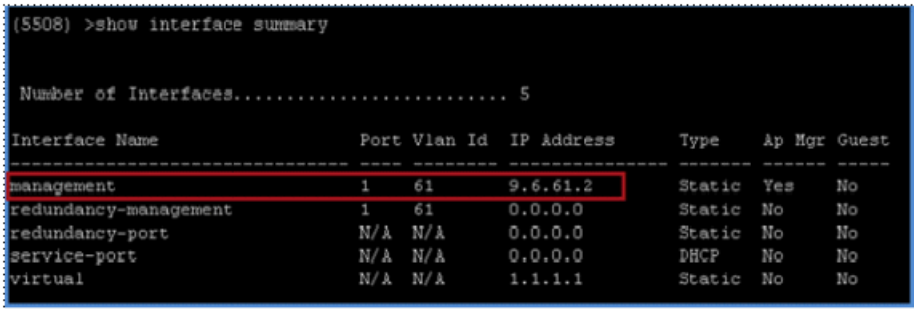


CLI からの HA の設定

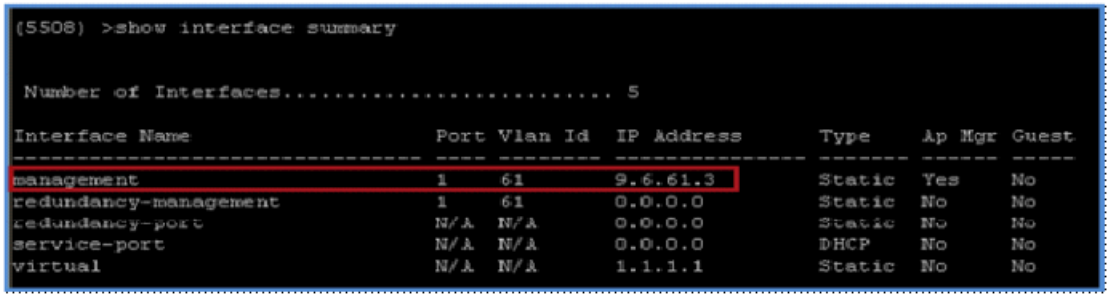
次の手順を実行します。

1. HA を設定する前に両方のコントローラの管理インターフェイスが同じサブネットに入っている必要があります。

   WLC 1:



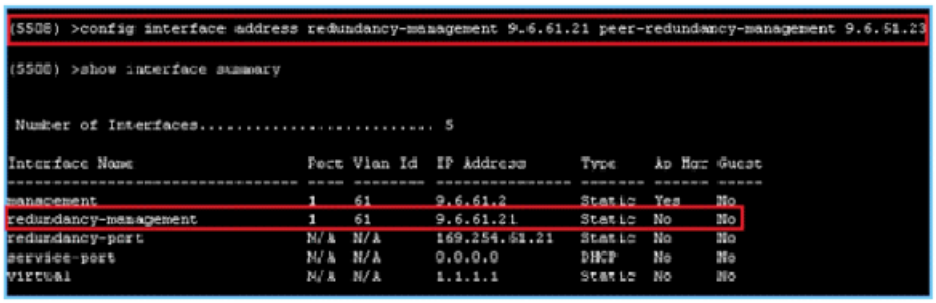
   WLC 2:



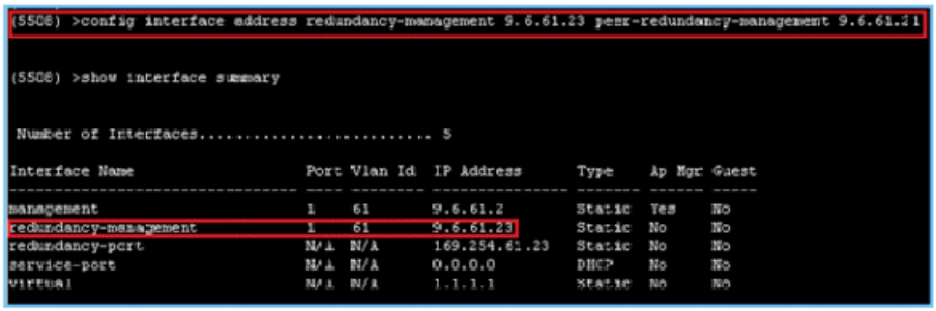
2. HA はデフォルトでディセーブルになっています。HA をイネーブルにする前に、冗長性管理 IP アドレスおよびピア冗長性管理 IP アドレスを設定する必要があります。両方のインターフェイスは、管理インターフェイスと同じサブネットにある必要があります。この例では、WLC 1 の冗長性管理 IP アドレスは 9.6.61.21、WLC 2 の冗長性管理 IP アドレスは 9.6.61.23 です。9.6.61.23 が WLC 2 の冗長性管理 IP アドレス、9.6.61.21 が WLC 1 の冗長性管理 IP アドレスになるように設定する必要もあります。

   冗長性およびピア冗長性管理 IP アドレスを設定するには次の CLI を使用します。

   WLC 1:

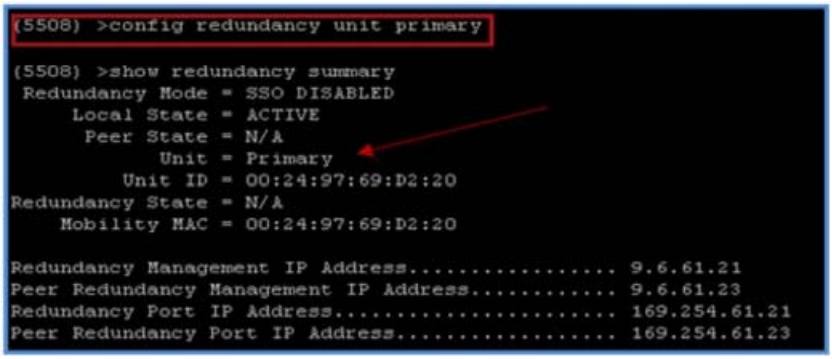


WLC 2:

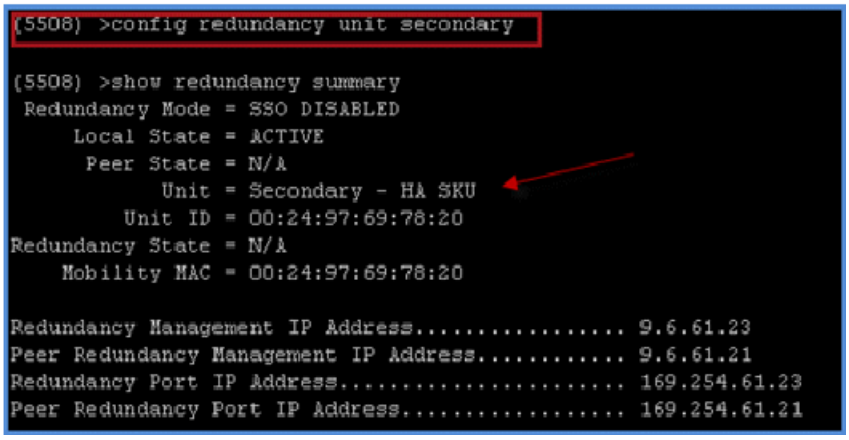


3. このステップの CLI を使用して、1 つの WLC をプライマリとして設定し(デフォルトでは、WLC HA ユニット ID がプライマリであり、有効な AP-BASE カウント ライセンスがインストールされている必要あり)、もう 1 つの WLC をセカンダリ(プライマリ WLC からの AP ベース カウントをこのユニットで継承)として設定します。この例では、WLC 1 がプライマリとして設定され、WLC 2 がセカンダリとして設定されています。

WLC 1:



WLC 2:



注: リリース 7.3 以降でオーダーできるファクトリ オーダー HA SKU の場合は、ユニットをセカンダリとして設定する必要はありません。ファクトリ オーダー HA SKU は、デフォルトのセカンダリ ユニットであり、有効な AP カウント ライセンスを持つアクティブ WLC と初めてペアにされたときに、スタンバイ WLC の役割を引き受けます。

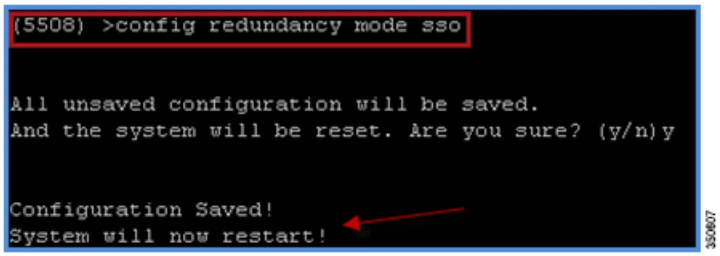
既存の任意の WLC をスタンバイ WLC として変換する場合は、CLI で config redundancy unit secondary コマンドを使用して変換します。この CLI コマンドは、スタンバイとして動作することが意図されている WLC に一定数の永久ライセンス カウントが備わっている場合に限り機能します。この条件は 5508 WLC だけに有効で、スタンバイに変換する最低 50 の AP 永久ライセンスが必要になります。5520、WiSM2、7500、および 8500 などの他の WLC に制約事項はありません。

4. WLC に冗長性管理とピア冗長性管理の IP アドレスを設定し終え、冗長ユニットを設定し終えたら、次に SSO をイネーブルにします。SSO をイネーブルにする前に、両方のコントローラ間の物理接続が存在しており(イーサネット ケーブルを使用し、冗長ポートを介して両方の WLC をバックツーバック接続)、アップリンクもインフラストラクチャ スイッチに接続されていて、両方の WLC からゲートウェイに到達可能であることを確認することが重要です。

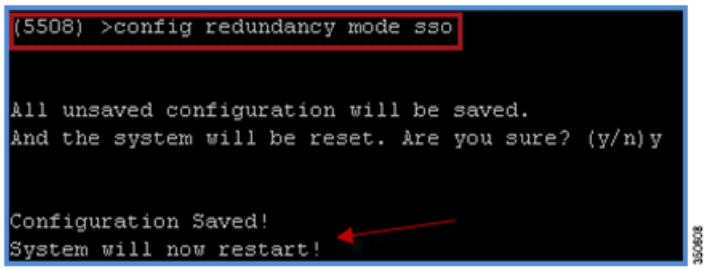
   SSO をイネーブルにすると、WLC がリブートされます。WLC では、ブート時に、設定に従い冗長ポートを介して HA 役割をネゴシエートします。WLC が冗長ポートを介するか冗長管理インターフェイスを介して相互に到達できない場合、セカンダリとして設定されている WLC はメンテナンス モードに遷移します。メンテナンス モードについては、このドキュメントで後述します。

5. このステップの CLI を使用して AP SSO をイネーブルにします。AP SSO をイネーブルにすると、WLC のリブートが開始されることに留意してください。

   WLC 1:



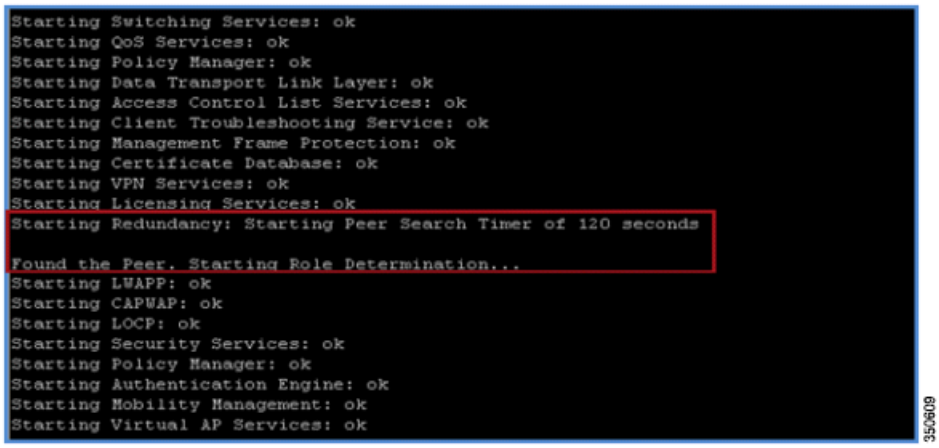
   WLC 2:



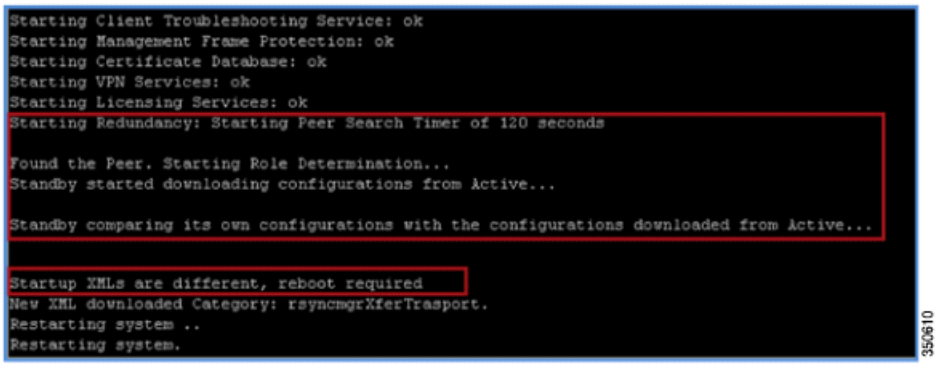
6. SSO をイネーブルにすると、実施した設定に従って HA 役割をネゴシエートするために WLC がリブートされます。役割が決定されると、冗長ポートを介してアクティブ WLC からスタンバイ WLC に設定が同期されます。最初に、セカンダリとして設定されている WLC が XML の不一致をレポートし、アクティブから設定をダウンロードして再度リブートします。セカンダリ WLC では、役割が決まった後の次回リブート時に設定を再度検証した上で XML の不致をレポートせず、スタンバイ WLC として動作するように処理を続行します。

   次に両方の WLC からの起動ログを示します。

WLC 1:

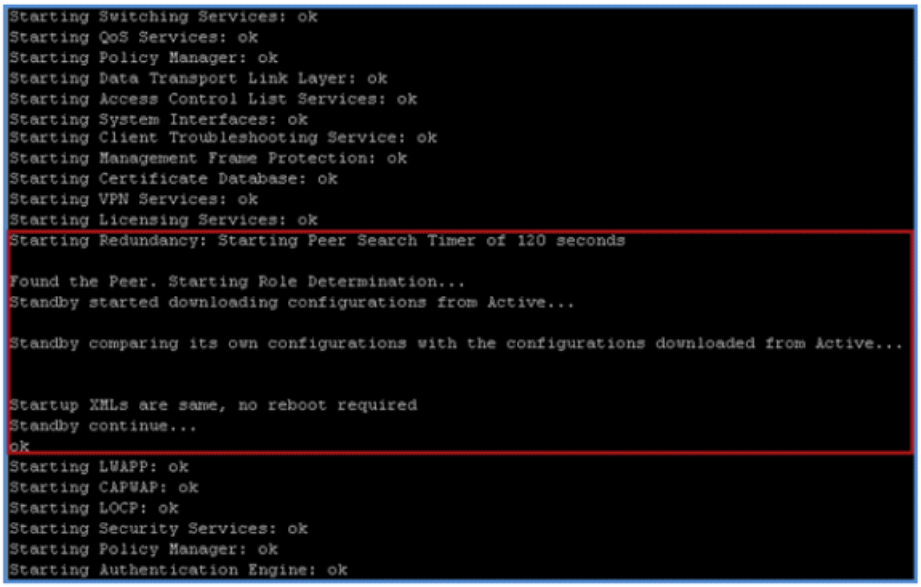


SSO をイネーブルにした後の最初の WLC 2 リブート:



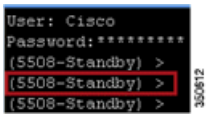
注:SSO をイネーブルにすると、コンソール接続またはサービス ポート上および冗長管理インターフェイス上の SSH からスタンバイ WLC にアクセスできます。

アクティブから XML 設定をダウンロードした後の WLC 2 の 2 度目のリブート:



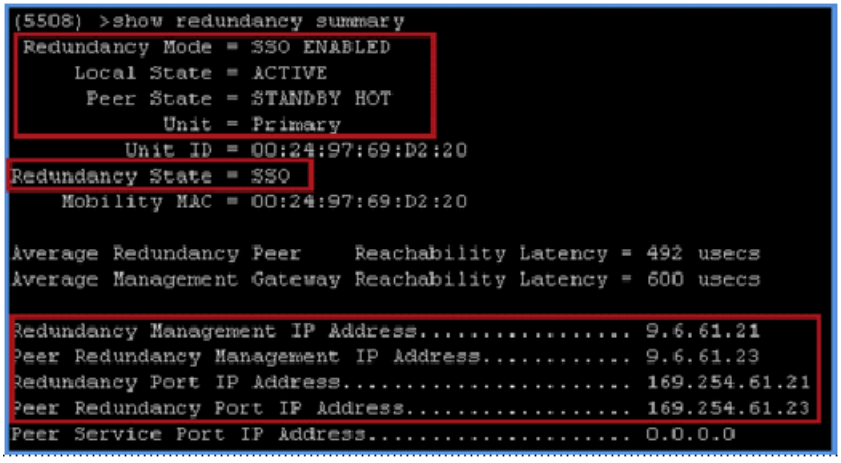
7. SSO をイネーブルにして WLC がリブートされ、XML 設定が同期されると、WLC 1 はアクティブ状態に遷移し、WLC 2 はスタンバイ ホット状態に遷移します。この時点以降は、すべての設定と管理をアクティブ WLC から実施する必要があるため、管理インターフェイス上の WLC 2 用の GUI、Telnet、SSH は機能しません。必要な場合、スタンバイ WLC(この例では WLC 2)は、コンソールまたはサービス ポートを介してのみ管理できます。

   また、ピア WLC がスタンバイ ホット状態に遷移すると、-Standby キーワードがスタンバイ WLC のプロンプト名に自動的に追加されます。

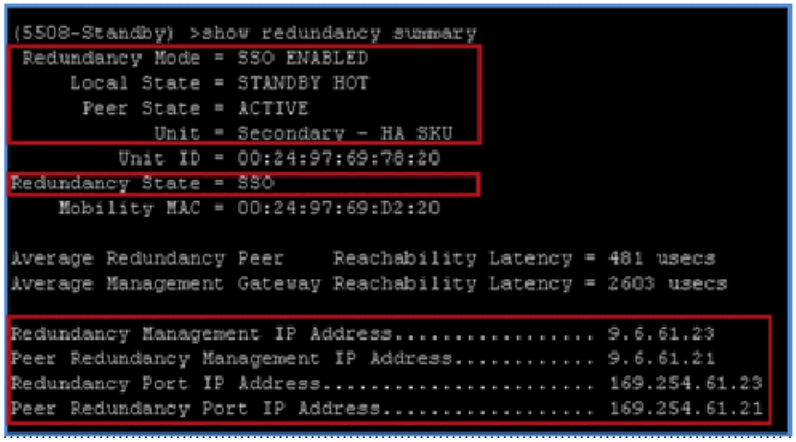


8. 次の手順を実行して、冗長性のステータスを確認します。

   a. WLC 1 の場合、[Monitor] > [Redundancy] > [Summary] と移動します。



b. WLC 2 の場合、コンソール接続に移動します。



注:SSO をイネーブルにすると、コンソール接続またはサービス ポート上および冗長管理インターフェイス上の SSH からスタンバイ WLC にアクセスできます。

HA ペアでの SSO の無効化

1. プライマリ コントローラで、次のコマンドを使用して SSO を無効にします。

Config redundancy mode disable

アクティブとスタンバイ WLC は、このコマンドが実行されるとリブートします。

スタンバイ コントローラは、リブート後に復帰すると、インターフェイスの IP アドレスがプライマリ コントローラと同じになり、すべてのポートが無効になります。

2. スタンバイ コントローラで、管理インターフェイスとダイナミック インターフェイスに対応する正しい IP アドレスを再入力し、次のコマンドを実行します。

Config port adminmode all enable

3. 設定をコントローラに保存します。
4. SSO を再度有効にするには、プライマリ コントローラとセカンダリ コントローラで **Config redundancy sso** コマンドを実行します。

両方のコントローラが再起動し、SSO モードでペアになります。スタンバイは、プライマリから設定を同期し、ホットスタンバイモードに戻ります。

GUI からの HA の設定

次の手順を実行します。

1. HA を設定する前に両方のコントローラの管理インターフェイスが同じサブネットに入っている必要があります。

WLC 1 と WLC 2:

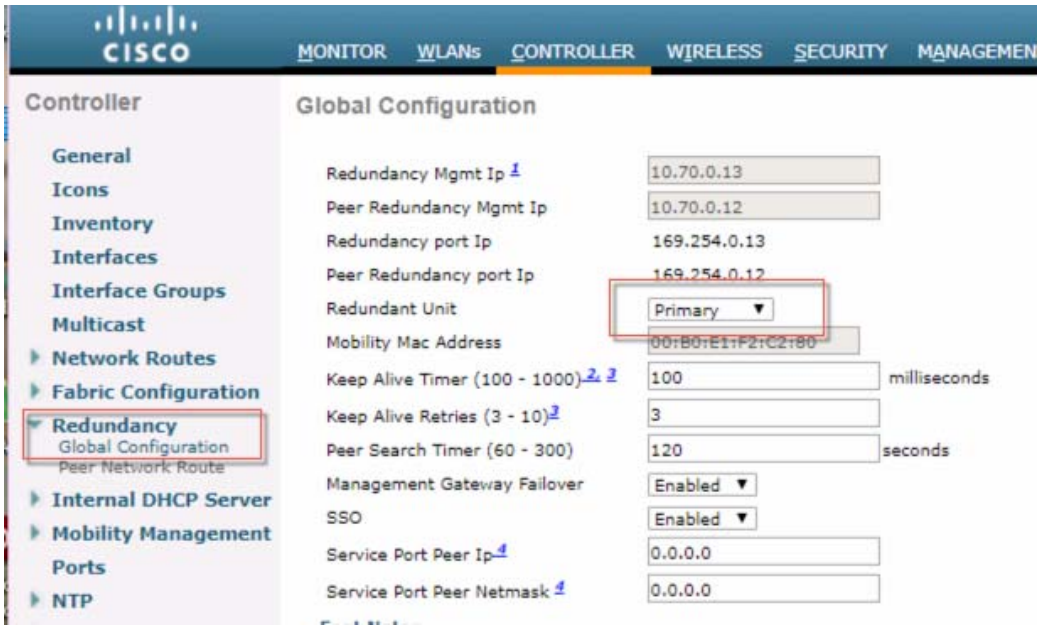
2. HA はデフォルトでディセーブルになっています。HA をイネーブルにする前に、冗長性管理 IP アドレスおよびピア冗長性管理 IP アドレスを設定する必要があります。

両方のインターフェイスは、管理インターフェイスと同じサブネットにある必要があります。この例では、WLC 1 の冗長性管理 IP アドレスは 10.70.0.12、WLC 2 の冗長性管理 IP アドレスは 10.70.0.13 です。WLC 2 で、10.70.0.13 が WLC 2 の冗長性管理 IP アドレス、10.70.0.12 が WLC 1 の冗長性管理 IP アドレスになるように設定する必要があります。

両方のインターフェイスの IP アドレスを入力し、[Apply] をクリックします。

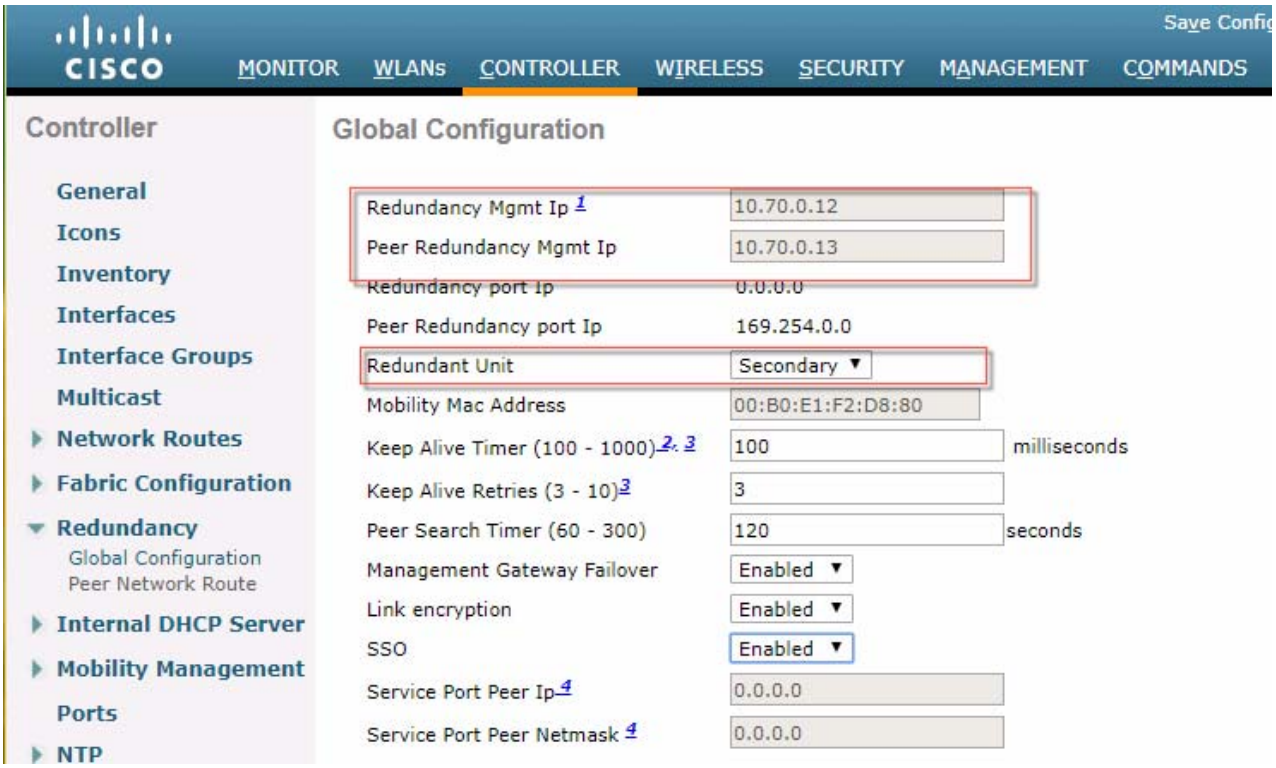
3. [Redundant Unit] ドロップダウン リストから、1 つの WLC を [Primary] に、もう 1 つの WLC を [Secondary] に設定します。この例では、WLC 1 が [Primary] として設定され、WLC 2 が [Secondary] として設定されています。設定が終わったら、[Apply] をクリックします。

WLC 1:



WLC 2:

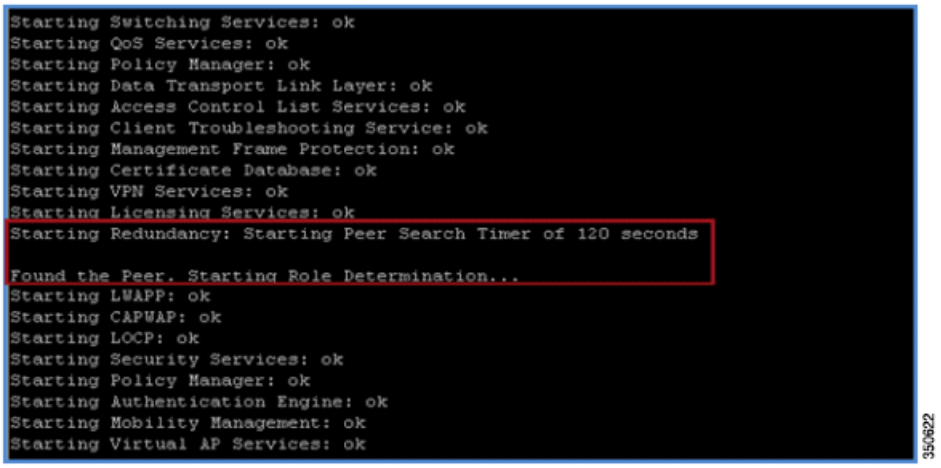
スタンバイ コントローラで、[Redundant Unit] に [Secondary] を設定します。



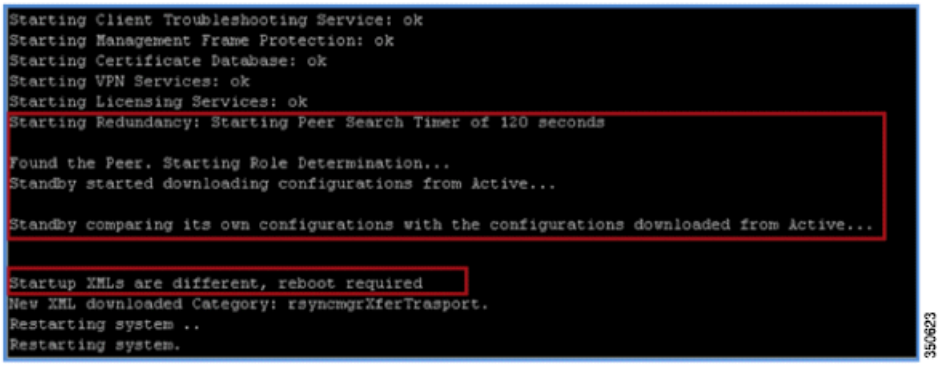
4. SSO をイネーブルにすると、実施した設定に従って HA 役割をネゴシエートするために WLC がリブートされます。役割が決定されると、冗長ポートを介してアクティブ WLC からスタンバイ WLC に設定が同期されます。最初に、セカンダリとして設定されている WLC が XML の不一致をレポートし、アクティブから設定をダウンロードして、再度リブートします。セカンダリ WLC では、役割が決まった後の次回リブート時に設定を再度検証した上で XML の不一致をレポートせず、スタンバイ WLC として機能するように処理を続行します。

   次に両方の WLC からの起動ログを示します。

   WLC 1：

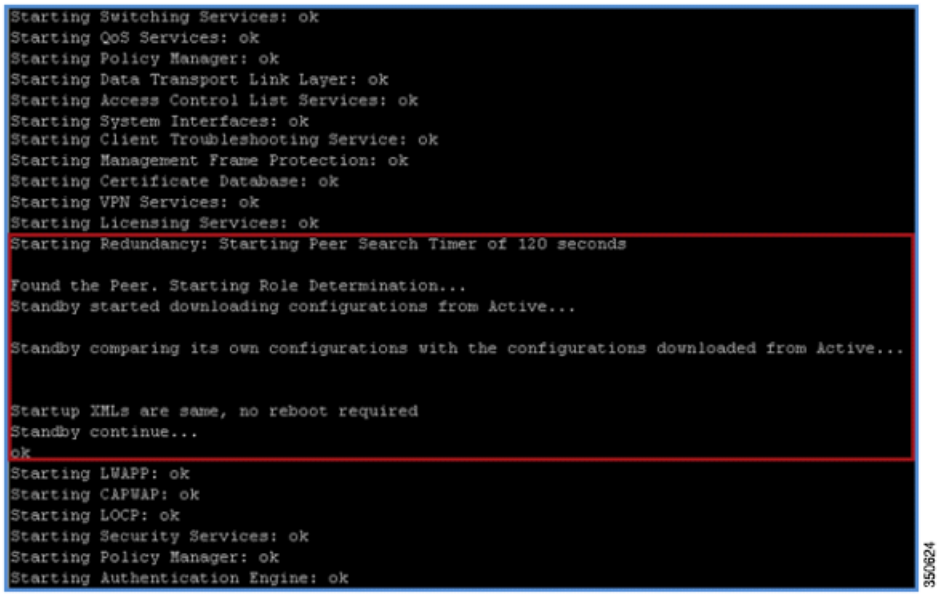


   SSO をイネーブルにした後の最初のリブート時の WLC：



   注：SSO をイネーブルにすると、コンソール接続またはサービス ポート上および冗長管理インターフェイス上の SSH からスタンバイ WLC にアクセスできます。

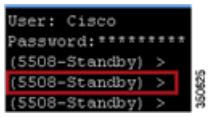
アクティブから XML 設定をダウンロードした後の WLC 2 の 2 度目のリブート:



5. SSO をイネーブルにして WLC がリブートされ、XML 設定が同期されると、WLC 1 の状態はアクティブに遷移し、WLC 2 の状態はスタンバイ ホットに遷移します。この時点以降は、すべての設定と管理をアクティブ WLC から実施する必要があるため、管理インターフェイス上の WLC 2 用の GUI、Telnet、SSH は機能しません。必要な場合、スタンバイ WLC(この場合は WLC 2)は、コンソールまたはサービス ポートを介してのみ管理できます。

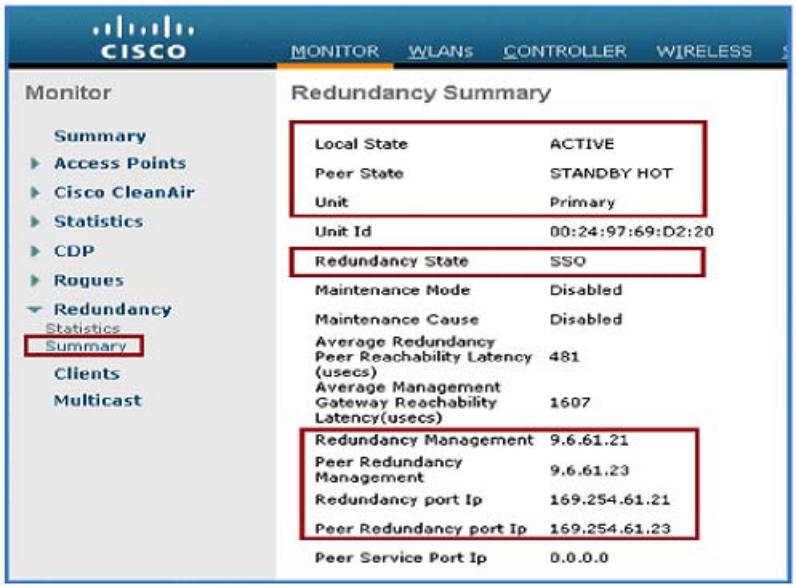
   また、ピア WLC がスタンバイ ホット状態に遷移すると、-Standby キーワードがスタンバイ WLC のプロンプト名に自動的に追加されます。

   注:プライマリを強制的にアクティブとして起動するには、プライマリ コントローラで HA をイネーブルにしてから 5 分後にセカンダリ コントローラで HA をイネーブルにします。

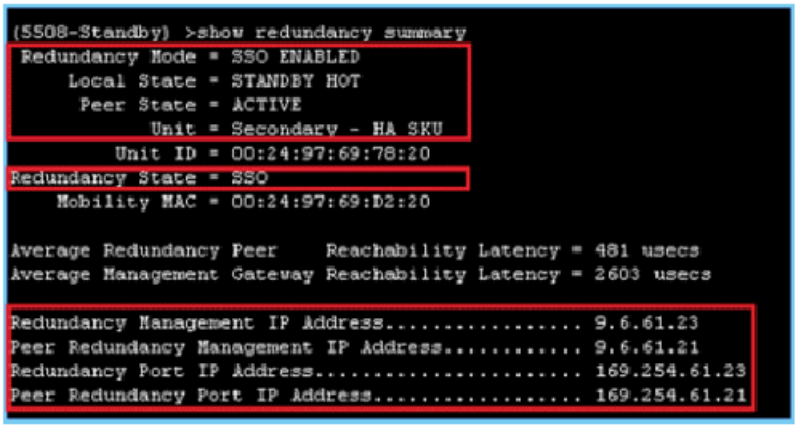


6. 次の手順を実行して、冗長性のステータスを確認します。

a. WLC 1 の場合、[Monitor] > [Redundancy] > [Summary] と移動します。



b. WLC 2 の場合、コンソール接続に移動します。

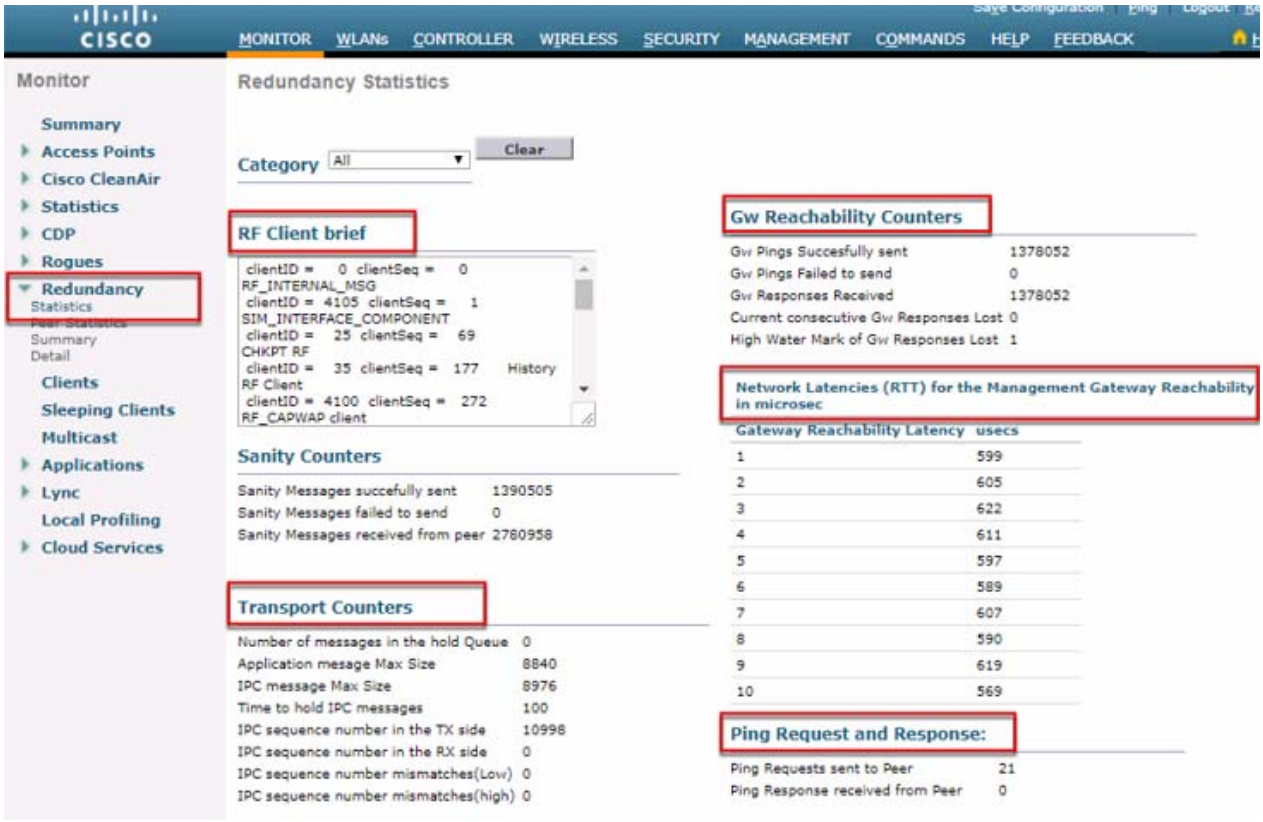


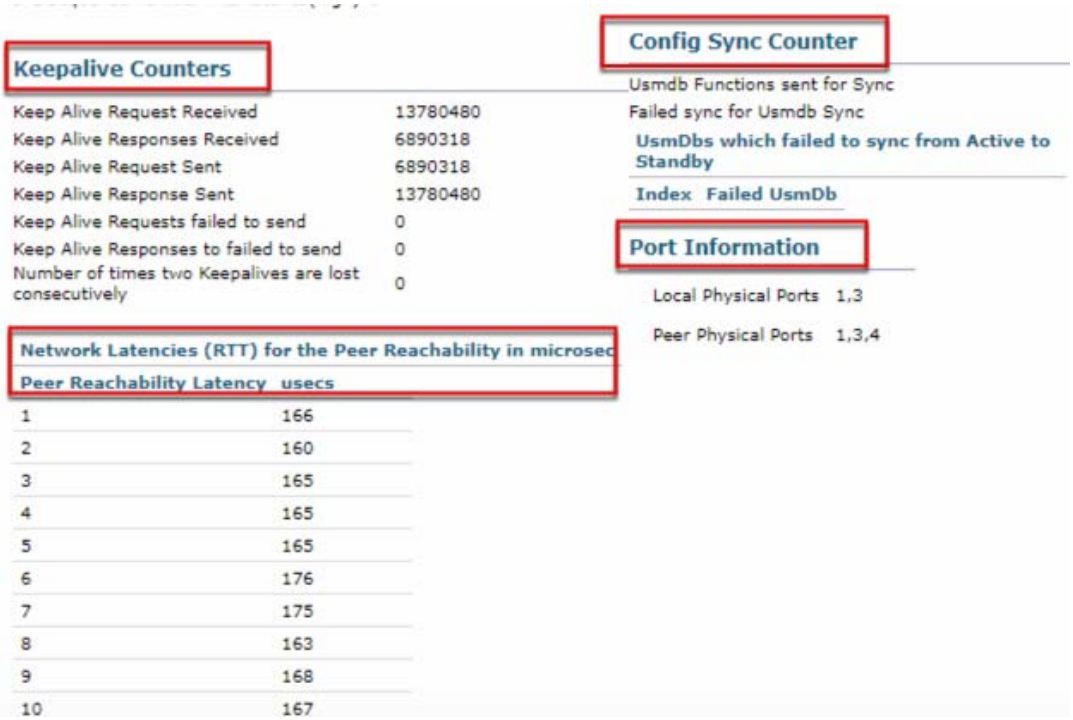
注:SSO をイネーブルにすると、コンソール接続またはサービス ポート上および冗長管理インターフェイス上の SSH からスタンバイ WLC にアクセスできます。

リリース 8.7 の HA 冗長性のモニタリング

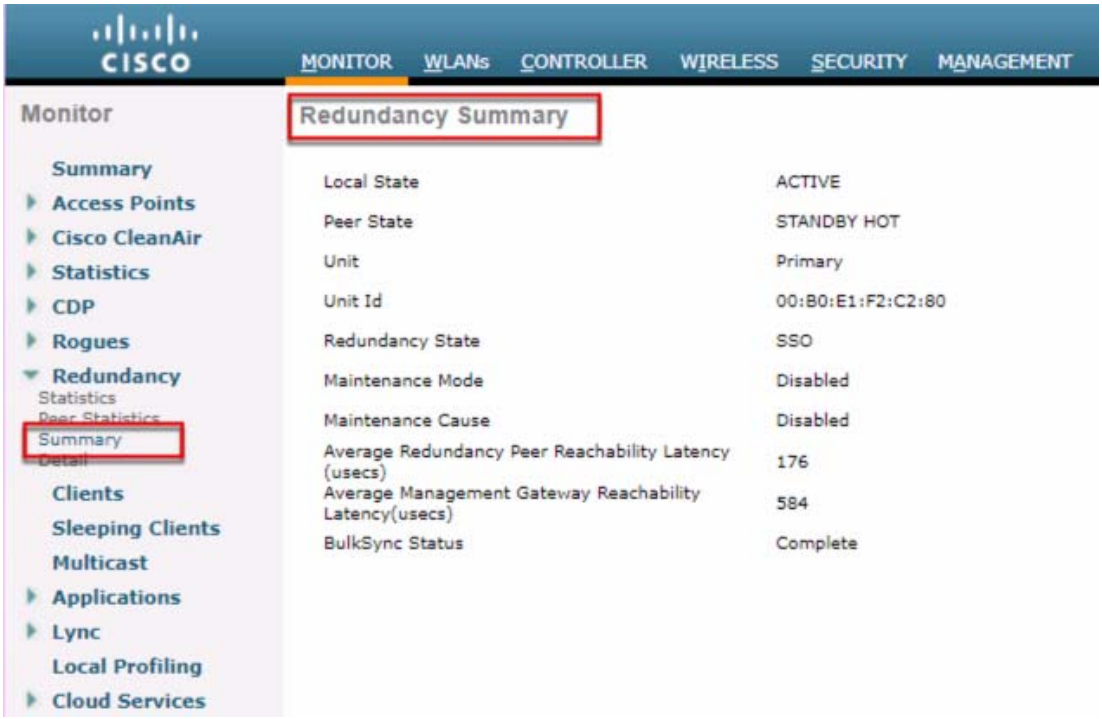
SNMP MIB を含む Management では、以下で説明する統計情報を取得するように **MIB CISCO-LWAPP-HA-MIB.my** が更新されています。

コントローラの [Monitor] タブに移動し、[Redundancy] を選択して**統計情報をモニタ**できます。

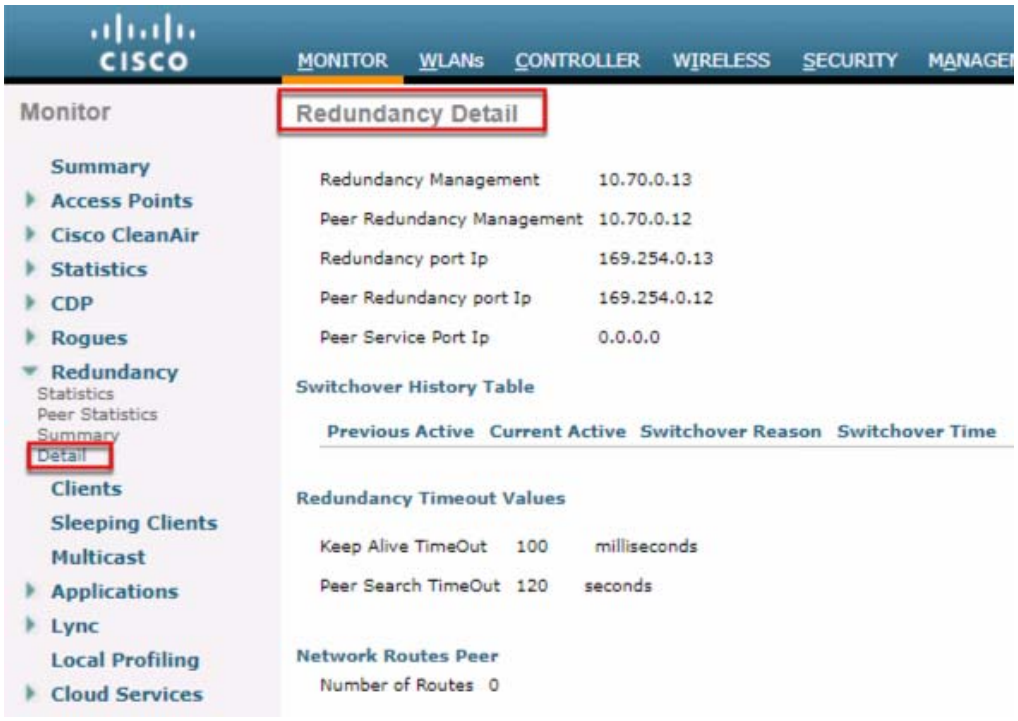

CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Redundancy
Statistics
Summary
Detail
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
Cloud Services
Redundancy Statistics
Category All
Clear
RF Client brief
clientID = 0 clientSeq = 0
RF_INTERNAL_MSG
clientID = 4105 clientSeq = 1
SIM_INTERFACE_COMPONENT
clientID = 25 clientSeq = 69
CHKPT RF
clientID = 35 clientSeq = 177 History
RF Client
clientID = 4100 clientSeq = 272
RF_CAPWAP client
Sanity Counters
Sanity Messages succefully sent 1390505
Sanity Messages failed to send 0
Sanity Messages received from peer 2780958
Transport Counters
Number of messages in the hold Queue 0
Application mesage Max Size 8840
IPC message Max Size 8976
Time to hold IPC messages 100
IPC sequence number in the TX side 10998
IPC sequence number in the RX side 0
IPC sequence number mismatches(Low) 0
IPC sequence number mismatches(high) 0
Gw Reachability Counters
Gw Pings Succesfully sent 1378052
Gw Pings Failed to send 0
Gw Responses Received 1378052
Current consecutive Gw Responses Lost 0
High Water Mark of Gw Responses Lost 1
Network Latencies (RTT) for the Management Gateway Reachability in microsec
Gateway Reachability Latency usecs
1 599
2 605
3 622
4 611
5 597
6 589
7 607
8 590
9 619
10 569
Ping Request and Response:
Ping Requests sent to Peer 21
Ping Response received from Peer 0

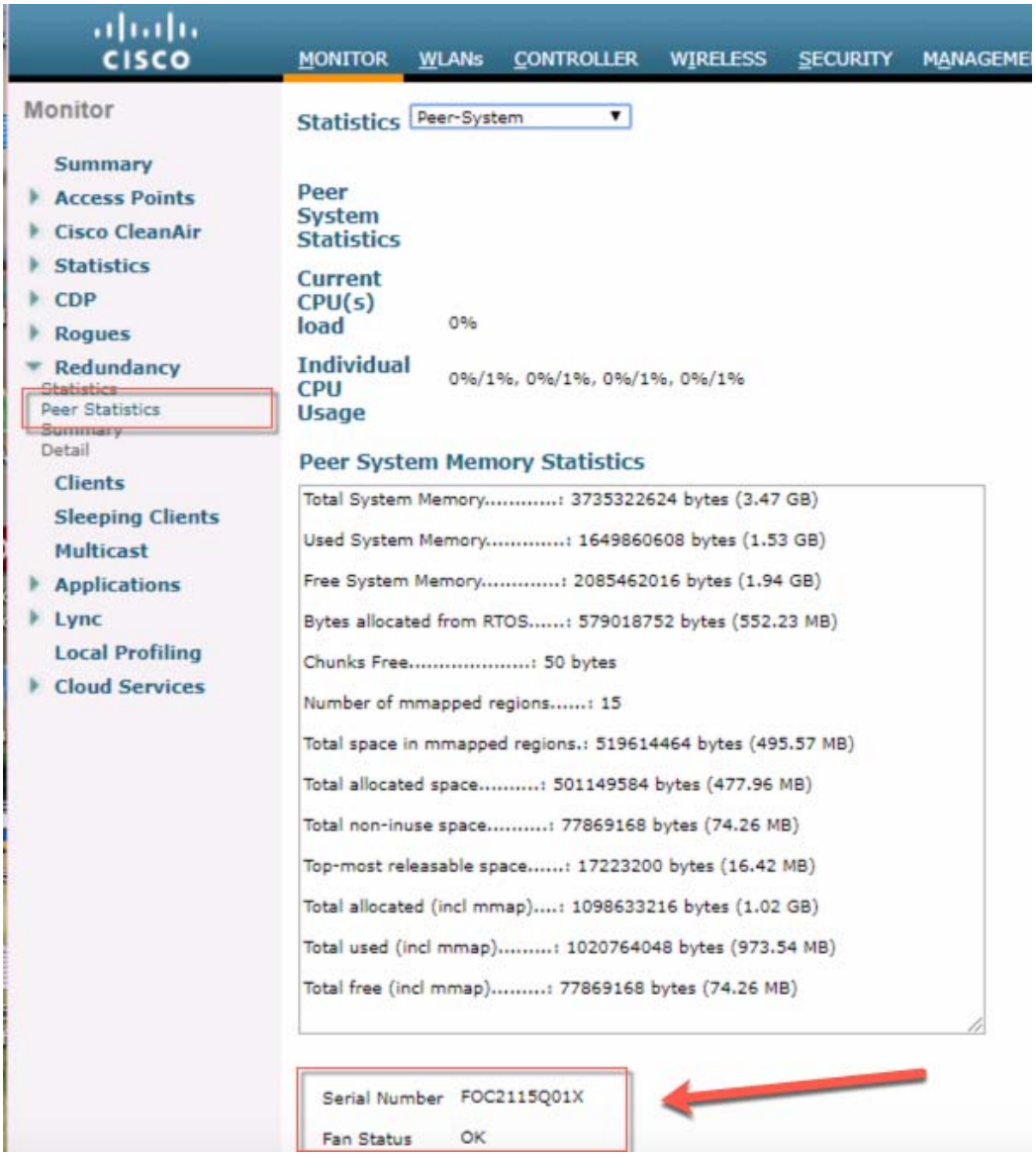

Keepalive Counters
Keep Alive Request Received 13780480
Keep Alive Responses Received 6890318
Keep Alive Request Sent 6890318
Keep Alive Response Sent 13780480
Keep Alive Requests failed to send 0
Keep Alive Responses to failed to send 0
Number of times two Keepalives are lost consecutively 0
Network Latencies (RTT) for the Peer Reachability in microsec
Peer Reachability Latency usecs
1 166
2 160
3 165
4 165
5 165
6 176
7 175
8 163
9 168
10 167
Config Sync Counter
Usmdb Functions sent for Sync
Failed sync for Usmdb Sync
UsmDbs which failed to sync from Active to Standby
Index Failed UsmDb
Port Information
Local Physical Ports 1,3
Peer Physical Ports 1,3,4

同じタブで、[Summary] を選択すると、アクティブ コントローラの [Redundancy Summary] を表示できます。



8.7 リリースで強化された新しい機能に、[Peer Statistics] があります。これには、ピアのシリアル番号およびファンのステータスに関する追加情報が表示されます。





次の CLI コマンドでも同じ情報を表示できます。

show redundancy peer-system statistics

```
(Cisco Controller) >show redundancy peer-system statistics
Peer System CPU statistics:Current CPU(s) load: 0%
Individual CPU load: 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%

Peer System Memory Statistics:
Total System Memory.....: 33163390976 bytes (30.88 GB)
Used System Memory.....: 3152162816 bytes (2.93 GB)
Free System Memory.....: 30011228160 bytes (27.95 GB)
Bytes allocated from RTOS.....: 832189248 bytes (793.69 MB)
Chunks Free.....: 71 bytes
Number of mmapped regions.....: 35
Total space in mmapped regions.: 1302372352 bytes (1.21 GB)
Total allocated space.....: 768079776 bytes (732.55 MB)
Total non-inuse space.....: 64109472 bytes (61.14 MB)
Top-most releasable space.....: 131216 bytes (128.14 KB)
Total allocated (incl mmap)....: 2134561600 bytes (1.98 GB)
Total used (incl mmap).....: 2070452128 bytes (1.92 GB)
Total free (incl mmap).....: 64109472 bytes (61.14 MB)

Peer system Power supply statistics:
Power Supply 1..... Present, OK
Power Supply 2..... Absent
Serial Number..... FCH1921V24U
Fan Status..... OK
```

コンフィギュレーション ウィザードからの HA の設定

次の手順を実行します。

1. 2 つの WLC 間の HA もコンフィギュレーション ウィザードからイネーブルにできます。HA をイネーブルにする前に、両方の WLC の管理 IP アドレスを同じサブネットに設定する必要があります。

   WLC 1:

```
System Name [Cisco_69:d2:24] (31 characters max): 5508
Enter Administrative User Name (24 characters max): Cisco
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password                  : *********

Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 10.10.10.10
Service Interface Netmask: 255.255.255.0

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 9.6.61.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 9.6.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 9.1.0.100
```

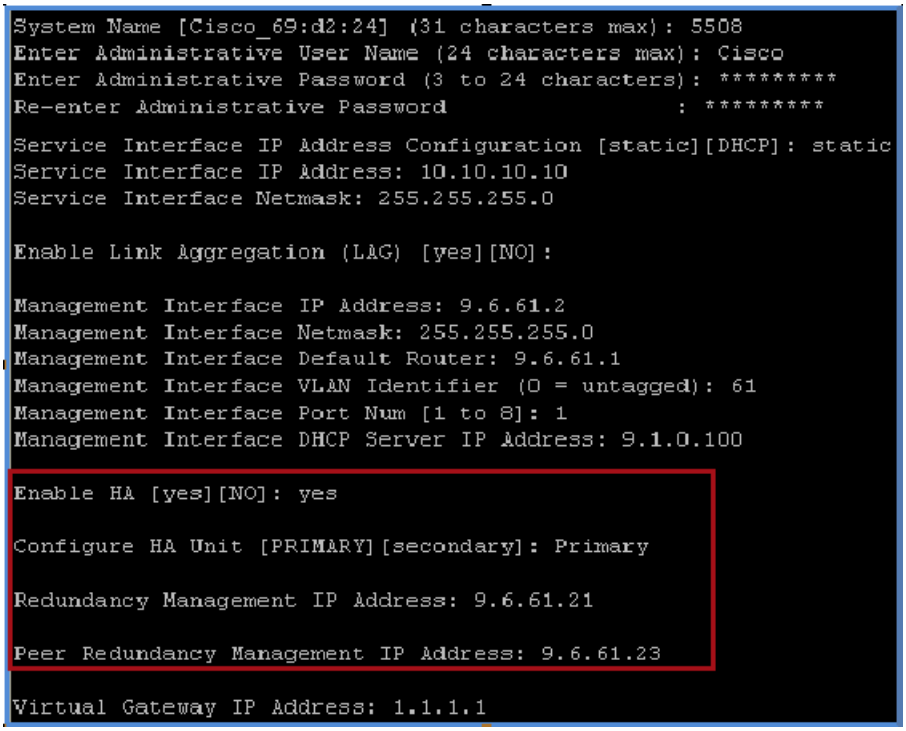
WLC 2:

```
System Name [Cisco_69:78:24] (31 characters max): 5508
Enter Administrative User Name (24 characters max): Cisco
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password                  : *********

Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 10.10.10.11
Service Interface Netmask: 255.255.255.0

Enable Link Aggregation (LAG) [yes][NO]:

Management Interface IP Address: 9.6.61.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 9.6.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 9.1.0.100
```

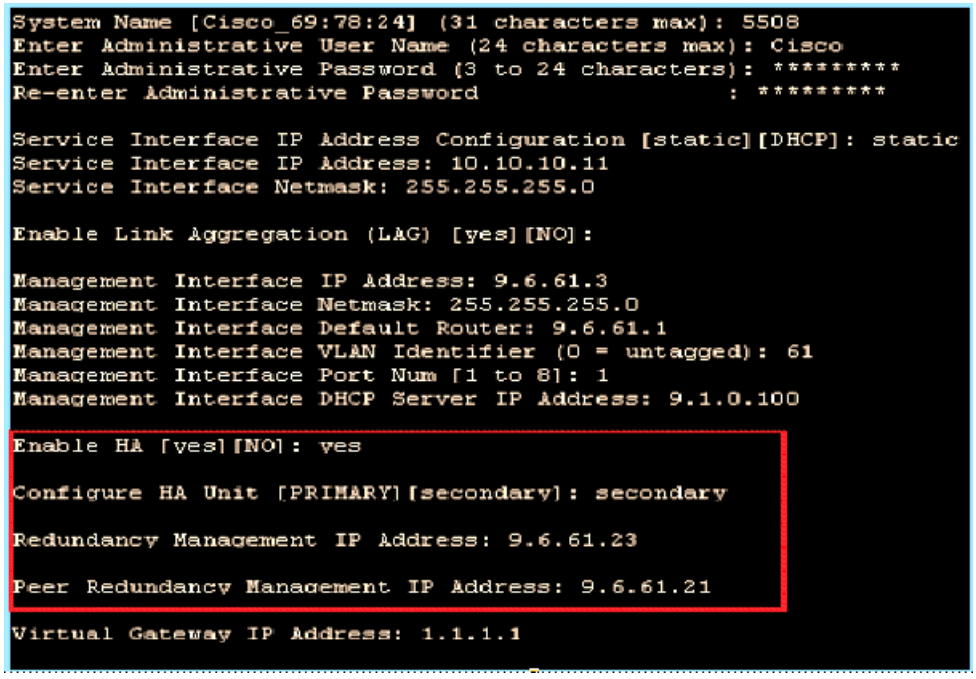
2. 管理 IP を設定すると、HA をイネーブルにするよう、ウィザードからメッセージが表示されます。HA をイネーブルにするには yes を入力します。その場合は、続いて、プライマリとセカンダリ ユニットおよび冗長性管理とピア管理の IP アドレスを設定します。

   - この例では、WLC 1 をプライマリ WLC として設定し、これがアクティブ WLC の役割を引き受けます。WLC 2 はセカンダリとして設定され、スタンバイ WLC の役割を引き受けます。
   - プライマリとセカンダリのユニットの入力後に、冗長性管理 IP アドレスおよびピア冗長性管理 IP アドレスを設定する必要があります。両方のインターフェイスは、管理インターフェイスと同じサブネットにある必要があります。この例では、WLC 1 の冗長性管理 IP アドレスは 9.6.61.21、WLC 2 の冗長性管理 IP アドレスは 9.6.61.23 です。WLC 2 で、9.6.61.23 が WLC 2 の冗長性管理 IP アドレス、9.6.61.21 が WLC 1 の冗長性管理 IP アドレスになるように設定する必要があります。

WLC 1:


System Name [Cisco_69:d2:24] (31 characters max): 5508
Enter Administrative User Name (24 characters max): Cisco
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password : *********
Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 10.10.10.10
Service Interface Netmask: 255.255.255.0
Enable Link Aggregation (LAG) [yes][NO]:
Management Interface IP Address: 9.6.61.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 9.6.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 9.1.0.100
Enable HA [yes][NO]: yes
Configure HA Unit [PRIMARY][secondary]: Primary
Redundancy Management IP Address: 9.6.61.21
Peer Redundancy Management IP Address: 9.6.61.23
Virtual Gateway IP Address: 1.1.1.1

WLC 2:


System Name [Cisco_69:78:24] (31 characters max): 5508
Enter Administrative User Name (24 characters max): Cisco
Enter Administrative Password (3 to 24 characters): *********
Re-enter Administrative Password : *********
Service Interface IP Address Configuration [static][DHCP]: static
Service Interface IP Address: 10.10.10.11
Service Interface Netmask: 255.255.255.0
Enable Link Aggregation (LAG) [yes][NO]:
Management Interface IP Address: 9.6.61.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 9.6.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 9.1.0.100
Enable HA [yes][NO]: yes
Configure HA Unit [PRIMARY][secondary]: secondary
Redundancy Management IP Address: 9.6.61.23
Peer Redundancy Management IP Address: 9.6.61.21
Virtual Gateway IP Address: 1.1.1.1

3. コンフィギュレーション ウィザードから HA をイネーブルにした後で、続けて、次のレガシー ウィザード パラメータを設定します。

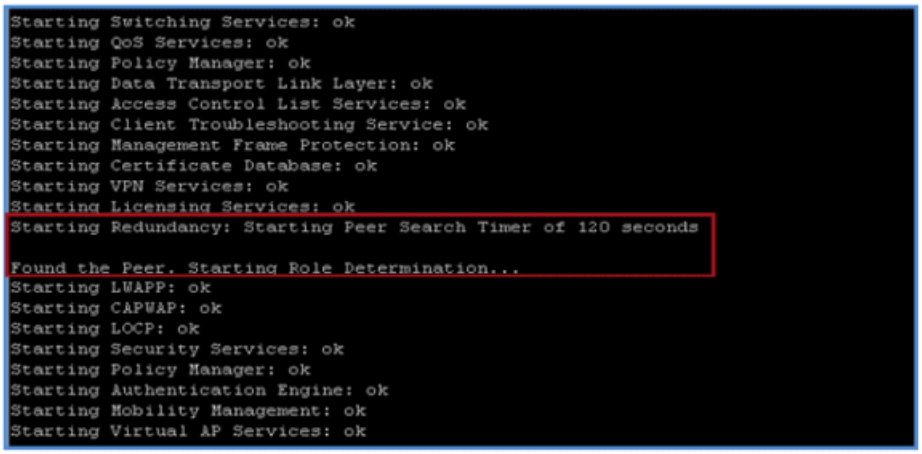
   - 仮想 IP アドレス
   - モビリティ ドメイン名
   - SSID
   - DHCP ブリッジ モード
   - RADIUS の設定
   - 国番号
   - NTP 設定など

   最後まで進んで設定を保存すると、WLC がリブートします。

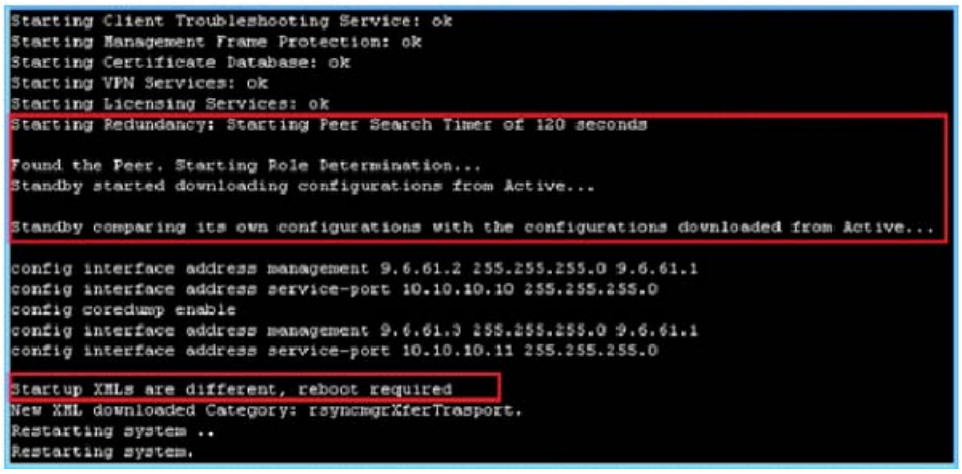
4. WLC では、ブート時に、実施した設定に従って HA 役割をネゴシエートします。役割が決定されると、冗長ポートを介してアクティブ WLC からスタンバイ WLC に設定が同期されます。最初に、セカンダリとして設定されている WLC が XML の不一致をレポートし、アクティブから設定をダウンロードして、再度リブートします。セカンダリ WLC では、役割が決まった後の次回リブート時に設定を再度検証した上で XML の不一致をレポートせず、スタンバイ WLC として動作するように処理を続行します。

   次に両方の WLC からの起動ログを示します。

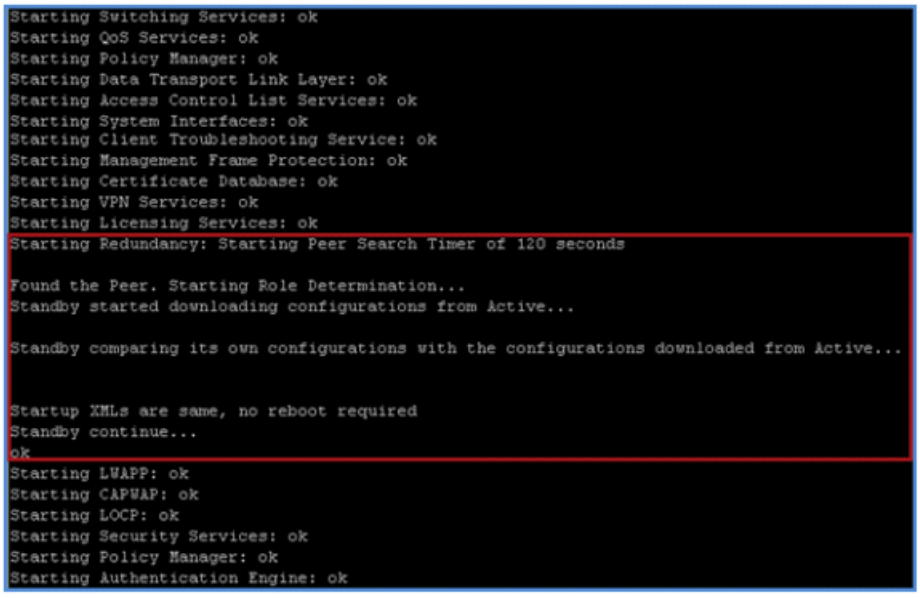
   WLC 1:



HA をイネーブルにした後の最初の WLC 2 リブート:



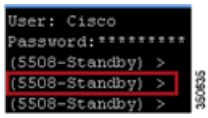
アクティブから XML 設定をダウンロードした後の WLC 2 の 2 度目のリブート:



注:SSO をイネーブルにすると、コンソール接続またはサービス ポート上および冗長管理インターフェイス上の SSH からスタンバイ WLC にアクセスできます。

5. HA をイネーブルにし、WLC がリブートして XML 設定が同期されると、WLC 1 はアクティブ状態に遷移し、WLC 2 はスタンバイ ホット状態に遷移します。この時点以降は、すべての設定と管理をアクティブ WLC から実施する必要があるため、管理インターフェイス上の WLC 2 用の GUI、Telnet、SSH は機能しません。必要な場合、スタンバイ WLC(この場合は WLC 2)は、コンソールまたはサービス ポートを介してのみ管理できます。

   また、ピア WLC がスタンバイ ホット状態に遷移すると、-Standby キーワードがスタンバイ WLC のプロンプト名に自動的に追加されます。



6. 次の手順を実行して、冗長性のステータスを確認します。

   a. WLC 1 の場合:

```
(5508) >show redundancy summary
 Redundancy Mode = SSO ENABLED
     Local State = ACTIVE
      Peer State = STANDBY HOT
            Unit = Primary
         Unit ID = 00:24:97:69:D2:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 486 usecs
Average Management Gateway Reachability Latency = 2043 usecs

Redundancy Management IP Address.................. 9.6.61.21
Peer Redundancy Management IP Address............. 9.6.61.23
Redundancy Port IP Address........................ 169.254.61.21
Peer Redundancy Port IP Address................... 169.254.61.23
Peer Service Port IP Address...................... 10.10.10.11
```

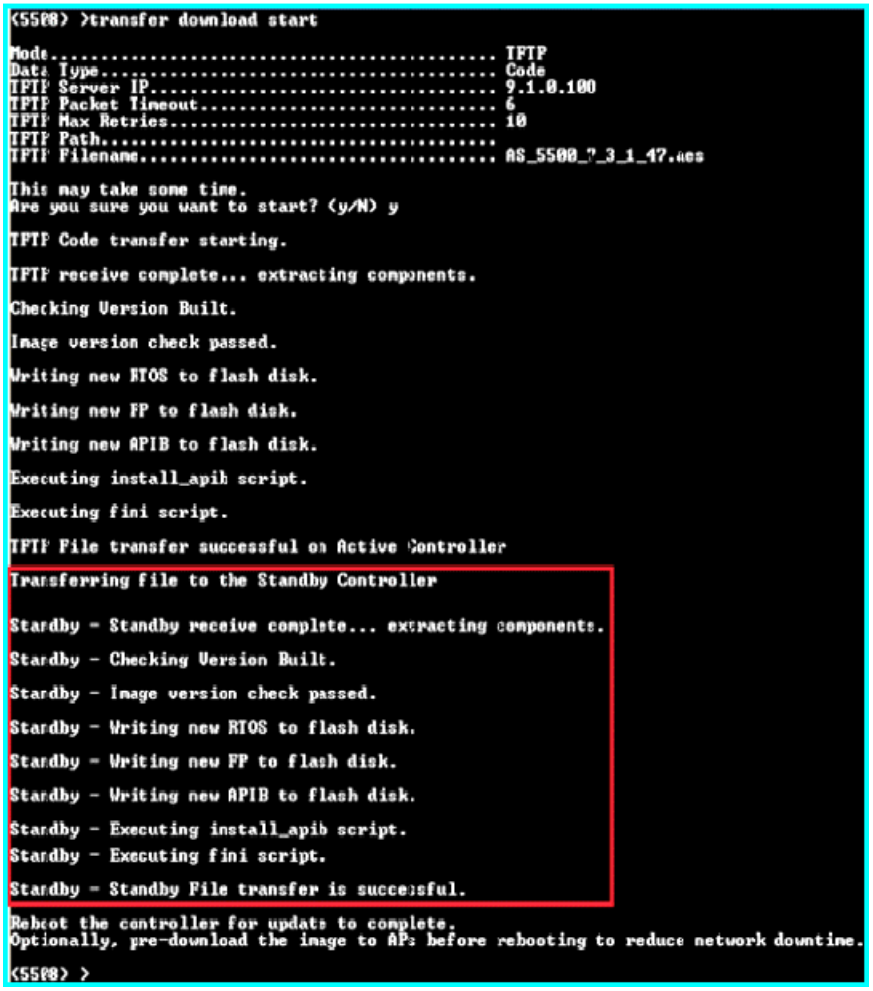
   b. WLC 2 の場合、コンソール接続に移動します。

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
     Local State = STANDBY HOT
      Peer State = ACTIVE
            Unit = Secondary - HA SKU
         Unit ID = 00:24:97:69:78:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 506 usecs
Average Management Gateway Reachability Latency = 676 usecs

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

注:SSO をイネーブルにすると、コンソール接続またはサービス ポート上および冗長管理インターフェイス上の SSH からスタンバイ WLC にアクセスできます。

HA セットアップの WLC のアップグレード

スタンバイ WLC を TFTP サーバまたは FTP サーバから直接アップグレードすることはできません。すべてのスクリプトの実行を終えると、アクティブ WLC がスタンバイ WLC にイメージを転送します。スタンバイ WLC は、アクティブ WLC からイメージを受信すると、アップグレード スクリプトの実行を開始します。イメージ転送とスタンバイ WLC 上でのスクリプト実行のすべてのログは、アクティブ WLC で参照できます。



注:FUS イメージは、コントローラで HA がイネーブルにされた状態でアップグレードできます。セカンダリ コントローラは通常のコードをアップグレードするときと同様にアップグレードされます。ただし、プライマリ コントローラでリブートを開始した場合、FUS のアップグレードが HA ペアのアクティブとスタンバイの両方で完了するまで、両方のコントローラが到達不能になります。このプロセスは、非 HA FUS のアップグレードと同様に、完了までに約 30 ～ 40 分かかります。

HA セットアップでのアップグレード手順

次の手順を実行します。

1. HA セットアップに WLC を設定した後は、TFTP サーバや FTP サーバからスタンバイ WLC を直接アップグレードできません。
2. CLI または GUI から HA セットアップのアクティブ WLC のアップグレードを開始し、アップグレードが完了するまで待ちます。
3. すべてのアップグレード スクリプトを実行し終えたアクティブ WLC では、冗長ポートを介してイメージ全体をスタンバイ WLC に転送します。

4. スタンバイ WLC は、アクティブ WLC からイメージを受信すると、アップグレード スクリプトの実行を開始します。スタンバイへのイメージの転送およびスタンバイ WLC でのアップグレード スクリプトの実行は、アクティブ WLC のコンソール、Telnet、SSH、HTTP 接続で参照できます。
5. スタンバイ アップグレードの正常終了を示すメッセージがアクティブ WLC に表示されたら、新しいイメージがプライマリ イメージとして設定されていることを確認するために、アクティブ WLC で show boot コマンドを発行することが重要です。
6. 確認できたら、ネットワーク内のすべての AP に新しいイメージを転送するために、アクティブ WLC でプライマリ イメージのプレダウンロードを開始します。
7. すべての AP でプレイメージが完了したら、show AP image all コマンドを発行して、WLC 上のプライマリ イメージが AP でバックアップ イメージとして設定されていることを確認します。
8. AP でプライマリとしてバックアップ イメージを交換するために、swap オプションを開始します。この実装では、WLC および AP のプライマリ イメージが新しいイメージに設定されます。
9. 新しいイメージでブートできるように AP および WLC をリセットするために、計画された停止に従って「no swap オプション」を付けた schedule-reset コマンドを発行します。
10. すべての AP はリブートし、新しいアクティブ WLC に接続します。
11. show boot、show sysinfo、show ap image all、および show redundancy summary コマンドを発行して、WLC と AP の両方が新しいイメージを使用してブートされていることを確認します。

HA セットアップに含まれる WLC のアップグレードを開始する前の重要なガイドライン

- サービス アップグレードはこのリリースではサポートされていません。したがって、HA セットアップの WLC をアップグレードする前にネットワーク停止時間を計画する必要があります。
- HA セットアップでのアップグレードを開始する前に、ピアがホット スタンバイ状態になっている必要があります。
- ソフトウェア バージョンの不一致がないように、アップグレード後に両方の WLC をほとんど同時にリブートすることをお勧めします。
- [Schedule Reset] は、HA セットアップの両方の WLC に適用されます。
- スケジュールされたリセットが計画されていない場合、スタンバイ WLC は、reset peer-system コマンドを使用してアクティブ WLC からリブートできます。
- デバッグ転送は、アクティブ WLC でもスタンバイ WLC でもイネーブルにできます。
- アクティブ WLC がダウンロードする際に突然再起動し、両方 WLC を再起動すると、アップグレードを実行する際は、WLC を再起動する必要があります。

HA セットアップでのファクトのダウンロードおよびアップロード

- スタンバイ WLC から設定を直接ダウンロードまたはアップロードすることはできません。
- イメージ、設定、Web 認証バンドル、署名ファイルなどすべてのタイプのダウンロード ファイルがまずアクティブ WLC にダウンロードされ、自動的にスタンバイ WLC にプッシュされます。
- アクティブ WLC にダウンロードされたコンフィギュレーション ファイルは、スタンバイ WLC にプッシュされます。この結果は、まずスタンバイ WLC がリセットされ、続いてアクティブ WLC がリセットされます。
- ピア サービス ポートおよびスタティック ルート設定は異なる XML ファイルの一部であり、コンフィギュレーション ファイルの一部としてダウンロードされても適用されません。
- 証明書のダウンロードは、各ボックスで別々に実行する必要があり、ペアリングの前に実行する必要があります。

- 設定、イベント ログ、クラッシュ ファイルなどのさまざまなファイル タイプのアップロードは、スタンバイ WLC から別々に実行できます。一方、サーバ IP、ファイル タイプ、パスと名前などアップロード用のさまざまなパラメータを設定するための CLI は、アクティブ WLC で実行する必要があります。アクティブ WLC でアップロード パラメータを設定し終えたら、スタンバイ WLC からのアップロードを開始するために、アクティブ WLC で `transfer upload peer-start` コマンドを発行する必要があります。

- サービス ポートの状態は、アクティブ WLC からスタンバイ WLC に同期されます。つまり、アクティブ WLC サービス ポートで DHCP がイネーブルにされている場合は、スタンバイ WLC でも DHCP を使用してサービス ポートの IP アドレスを取得します。アクティブ WLC のサービス ポートがスタティック IP アドレスを使用して設定されている場合は、スタンバイ WLC も別のスタティック IP アドレスを使用して設定する必要があります。スタンバイ WLC サービス ポートの IP アドレスを設定する CLI は、`configure redundancy interface address peer-service-port <IP Address>` です。このコマンドは、アクティブ WLC から実行する必要があります。また、スタンバイ WLC で、アウトオブバンド管理のためのルートをサービス ポートに設定するには、アクティブ WLC から `configure redundancy peer-route add <Network IP Address > <IP Mask> <Gateway>` コマンドを発行します。

HA セットアップでのフェールオーバー プロセス

HA セットアップでは、AP の CAPWAP 状態は、アクティブ WLC およびスタンバイ WLC で維持されます(Run 状態の AP に限る)。つまり、Up Time および Association Up Time は両方の WLC で維持され、スイッチオーバーが開始されるとスタンバイ WLC がネットワークを引き継ぎます。この例では、WLC 1 がアクティブ状態でネットワークを処理しており、WLC 2 がスタンバイ状態でアクティブ WLC をモニタしています。WLC 2 はスタンバイ状態ですが、まだ AP の CAPWAP 状態を維持します。

WLC 1:

```
(5508) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                Association Up Time
------------------  -----------------  ------------------------  ------------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 02 h 37 m 33 s    0 days, 02 h 36 m 22 s
```

350656

WLC 2:

```
(5508-Standby) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                Association Up Time
------------------  -----------------  ------------------------  ------------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 02 h 38 m 11 s    0 days, 02 h 37 m 00 s
```

350657

HA セットアップでの WLC フェールオーバーは、2 つの異なるセクションに分類できます。

ボックス フェールオーバー

ボックス フェールオーバー(アクティブ WLC のクラッシュ、システム ハング、手動リセット、強制スイッチオーバー)の場合は、冗長ポートを介してアクティブ WLC から直接コマンドが送信され、ネットワークを引き継ぐために冗長管理インターフェイスからスタンバイ WLC にも送信されます。この処理には、ネットワーク内の AP の数に応じて、5 ～ 100 ミリ秒かかります。アクティブ WLC の電源障害またはスイッチオーバーのための直接コマンドを送信できない何らかのクラッシュの場合は、ネットワーク内の AP の数に応じて 350 ～ 500 ミリ秒かかります。

アクティブ ボックスの電源障害の場合にフェールオーバーにかかる時間も WLC に設定されているキープアライブ タイマーに依存します(デフォルトでは 100 ミリ秒に設定)。フェールオーバーを決めるために使用されるアルゴリズムを次に示します。

- スタンバイ WLC はアクティブ WLC にキープアライブを送信し、デフォルト タイマーに従い 100 ミリ秒以内に確認応答があることを期待します。この時間は、100 ～ 400 ミリ秒の範囲で設定できます。
- 100 ミリ秒以内にキープアライブの確認応答がない場合、スタンバイ WLC では、ボックス フェールオーバーであるのか冗長ポート接続に関する何らかの問題であるのかを確認するために、冗長管理インターフェイスを介してアクティブ WLC に即座に ICMP メッセージを送信します。
- ICMP メッセージに対する応答がない場合、スタンバイ WLC は積極性を増してスタンバイ WLC に別のキープアライブ メッセージを即座に送信し、25 % 減らした時間(つまり、100 ミリ秒を 25 % 短くした 75 ミリ秒)以内の確認応答を期待します。
- 75 ミリ秒以内にキープアライブの確認応答がない場合、スタンバイ WLC は、冗長管理インターフェイスを介してアクティブ WLC に別の ICMP メッセージを即座に送信します。
- 同様に、2 つ目の ICMP メッセージに対する応答がない場合、スタンバイ WLC はさらに積極性を増し、別のキープアライブ メッセージを即座にスタンバイ WLC に送信して、最新のキープアライブ タイマーから実際のタイマーの 25 % をさらに削減した時間(つまり、最新のキープアライブ タイマー 75 ミリ秒から 100 ミリ秒の 25 % を短くした 50 ミリ秒)以内の確認応答を期待します。
- 50 ミリ秒以内に 3 つ目のキープアライブ パケットの確認応答がない場合、スタンバイ WLC は、冗長管理インターフェイスを介してアクティブ WLC に別の ICMP メッセージを即座に送信します。
- 最後に、3 つ目の ICMP パケットからの応答がない場合、スタンバイ WLC ではアクティブ WLC は停止していると宣言し、アクティブ WLC の役割を引き受けます。

ネットワーク フェールオーバー

ネットワーク フェールオーバー(つまり、何らかの理由によりアクティブ WLC がゲートウェイに到達不能)の場合は、ネットワーク内の AP の数に応じてスイッチオーバーの完了まで 3 ～ 4 秒かかることがあります。

ボックス フェールオーバーのシミュレート手順

次の手順を実行します。

1. 設定のセクションで説明されている手順を実行して 2 つの WLC 間に HA を設定し、強制スイッチオーバーが開始される前に、両方の WLC がアクティブ WLC とスタンバイ WLC としてペアになっていることを確認します。

   WLC 1 の場合:

```
(5508) >show redundancy summary
Redundancy Mode = SSO ENABLED
     Local State = ACTIVE
      Peer State = STANDBY HOT
            Unit = Primary
         Unit ID = 00:24:97:69:D2:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer    Reachability Latency = 486 usecs
Average Management Gateway Reachability Latency = 2043 usecs

Redundancy Management IP Address.................. 9.6.61.21
Peer Redundancy Management IP Address............. 9.6.61.23
Redundancy Port IP Address........................ 169.254.61.21
Peer Redundancy Port IP Address................... 169.254.61.23
Peer Service Port IP Address...................... 10.10.10.11
```

WLC 2 の場合、コンソール接続に移動します。

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
      Local State = STANDBY HOT
       Peer State = ACTIVE
             Unit = Secondary - HA SKU
          Unit ID = 00:24:97:69:78:20
Redundancy State = SSO
    Mobility MAC = 00:24:97:69:D2:20

Average Redundancy Peer     Reachability Latency = 506 usecs
Average Management Gateway Reachability Latency = 676 usecs

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

2. AP を WLC に関連付け、両方の WLC で AP のステータスを確認します。HA セットアップでは、AP データベースのミラー コピーが両方の WLC で維持されます。つまり、AP の CAPWAP 状態がアクティブとスタンバイの WLC で維持され(Run 状態の AP に限る)、スイッチオーバーが開始されるとスタンバイ WLC がネットワークを引き継ぎます。この例では、WLC 1 がアクティブ WLC、WLC 2 がスタンバイ状態であり、AP データベースは両方の WLC で維持されています。

WLC 1:

```
(5508) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC       Location         Port  Country  Priority
------------------  -----  -------------------  -----------------  ---------------  ----  -------  --------
AP_3500E            2      AIR-CAP3502E-A-K9    c4:7d:4f:3a:07:74  [redacted]       1     [redacted]     1

(5508) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                Association Up Time
------------------  -----------------  ------------------------  ------------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 04 h 27 m 55 s    0 days, 04 h 26 m 44 s
```

350660

WLC 2

```
(5508-Standby) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC       Location         Port  Country  Priority
------------------  -----  -------------------  -----------------  ---------------  ----  -------  --------
AP_3500E            2      AIR-CAP3502E-A-K9    c4:7d:4f:3a:07:74  [redacted]       1     [redacted]     1

(5508-Standby) >show ap uptime

Number of APs.................................... 1
Global AP User Name.............................. cisco
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                Association Up Time
------------------  -----------------  ------------------------  ------------------------
AP_3500E            c4:7d:4f:3a:07:74  0 days, 04 h 29 m 07 s    0 days, 04 h 27 m 56 s
```

350661

3. オープンな WLAN を作成し、クライアントを関連付けます。クライアント データベースはスタンバイ WLC で同期されないため、クライアント エントリはスタンバイ WLC には存在しません。WLAN をアクティブ WLC に作成すると、この WLAN も冗長ポートを介してスタンバイ WLC に同期されます。

   WLC 1:

```
(5508) >show wlan summary

Number of WLANs.............................. 1

WLAN ID  WLAN Profile Name / SSID                Status    Interface Name        PMIPv6 Mobility
-------  ---------------------------------       --------  --------------------  ---------------
1        Beta-Test / Beta-Test                   Enabled   management            none

(5508) >show client summary

Number of Clients............................ 1

Number of PMIPV6 Clients..................... 0

MAC Address       AP Name           Status        WLAN/GLAN/RLAN Auth Protocol         Port Wired PMIPV6
----------------- ----------------- ------------- -------------- ---- ---------------- ---- ----- ------

00:40:96:b8:d4:be AP_3500E          Associated    1              Yes  802.11a          1    No    No
```

350662

   WLC 2:

```
(5508-Standby) >show wlan summary

Number of WLANs.............................. 1

WLAN ID  WLAN Profile Name / SSID                Status    Interface Name        PMIPv6 Mobility
-------  ---------------------------------       --------  --------------------  ---------------
1        Beta-Test / Beta-Test                   Enabled   management            none

(5508-Standby) >show client summary

Number of Clients............................ 0
```

350939

4. アクティブ WLC で redundancy force-switchover コマンドを発行します。このコマンドを発行すると、アクティブ WLC がリブートしてスタンバイ WLC がネットワークを引き継ぐ手動スイッチオーバーがトリガーされます。この場合、アクティブ WLC 上のクライアントは認証解除され、新しいアクティブ WLC に接続し直します。

   WLC 1:

```
(5508) >redundancy force-switchover

This will reload the active unit and force a switch of activity. Are you sure? (y/N) y


System will now restart!
```

350664

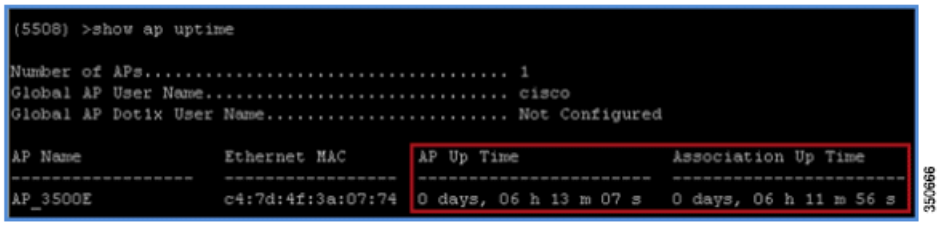
   WLC 2:

```
(5508-Standby) >
HA completed successfully. WLC switch over detection time : 0 msec and  APs switch over time : 1 msec
(5508) >show client summary

Number of Clients............................ 1

Number of PMIPV6 Clients..................... 0

MAC Address       AP Name           Status        WLAN/GLAN/RLAN Auth Protocol         Port Wired PMIPV6
----------------- ----------------- ------------- -------------- ---- ---------------- ---- ----- ------

00:40:96:b8:d4:be AP_3500E          Associated    1              Yes  802.11a          1    No    No
```

350665

   注: この例では、プロンプトが 5508-Standby から 5508 に変わります。これは、この WLC がアクティブ WLC になったためであり、AP スイッチオーバーにかかった時間は 1 ミリ秒です。

WLC 2:



当初スタンバイ WLC になっていて、スイッチオーバー後にアクティブ WLC になった WLC 2 の AP の CAPWAP 状態を確認してください。AP Up Time および Association Up Time が維持されており、AP は Discovery 状態になりませんでした。

次のマトリクスを参照すると、WLC スイッチオーバーのトリガー条件がはっきりとわかります。

ネットワークの問題					
RP ポート ステータス	冗長管理を介してピアに到達可能	アクティブからゲートウェイに到達可能	スタンバイからゲートウェイに到達可能	スイッチオーバー	結果
Up	Yes	Yes	Yes	No	アクションなし
Up	Yes	Yes	No	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。
Up	Yes	No	Yes	Yes	スイッチオーバー発生
Up	Yes	No	No	No	アクションなし
Up	No	Yes	Yes	No	アクションなし
Up	No	Yes	No	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。
Up	No	No	Yes	Yes	スイッチオーバー発生
Up	No	No	No	No	アクションなし
Down	Yes	Yes	Yes	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。
Down	Yes	Yes	No	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。
Down	Yes	No	Yes	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。

ネットワークの問題					
RP ポート ステータス	冗長管理を介してピアに到達可能	アクティブからゲートウェイに到達可能	スタンバイからゲートウェイに到達可能	スイッチオーバー	結果
Down	Yes	No	No	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。
Down	No	Yes	Yes	Yes	スイッチオーバーが発生し、ネットワークが競合状態になることがあります。
Down	No	Yes	No	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。
Down	No	No	Yes	Yes	スイッチオーバー発生
Down	No	No	No	No	スタンバイがリブートし、ゲートウェイの到達可能性を確認します。まだ到達可能でない場合は、メンテナンス モードに入ります。

システムに関する問題				
トリガー	RP ポート ステータス	冗長管理を介してピアに到達可能	スイッチオーバー	結果
CP のクラッシュ	Yes	No	Yes	スイッチオーバー発生
DP のクラッシュ	Yes	No	Yes	スイッチオーバー発生
システム ハング	Yes	No	Yes	スイッチオーバー発生
手動リセット	Yes	No	Yes	スイッチオーバー発生
強制スイッチオーバー	Yes	No	Yes	スイッチオーバー発生
CP のクラッシュ	No	Yes	Yes	スイッチオーバー発生

システムに関する問題				
トリガー	RP ポート ステータス	冗長管理を介してピアに到達可能	スイッチオーバー	結果
DP のクラッシュ	No	Yes	Yes	スイッチオーバー発生
システム ハング	No	Yes	Yes	スイッチオーバー発生
手動リセット	No	Yes	Yes	スイッチオーバー発生
強制スイッチオーバー	No	Yes	Yes	スイッチオーバー発生
CP のクラッシュ	No	No	Yes	「ネットワークの問題」セクションに従い更新
DP のクラッシュ	No	No	Yes	「ネットワークの問題」セクションに従い更新
システム ハング	No	No	Yes	「ネットワークの問題」セクションに従い更新
手動リセット	No	No	Yes	「ネットワークの問題」セクションに従い更新
強制スイッチオーバー	No	No	Yes	「ネットワークの問題」セクションに従い更新

HA ファクト

- HA ペアリングは、同じタイプのハードウェアとソフトウェア バージョンの間でだけ可能です。不一致があると、メンテナンスモードが開始されることがあります。SSO を設定する前に、両方の WLC で仮想 IP アドレスが同一である必要があります。
- 3500、5500、8500 シリーズの WLC の場合は、アクティブとスタンバイの冗長ポートの直接接続をお勧めします。
- WiSM-2 WLC は、同じ 6500 シャーシに設置する必要がありますが、パフォーマンスの信頼性を高めるために VSS セットアップに設置することもできます。
- HA 設定に先立って、冗長ポートとインフラストラクチャ ネットワークの間を物理的に接続する必要があります。

- 別の HA セットアップまたは独立したコントローラとのモビリティ ピアを形成するために、プライマリ ユニットの MAC を HA セットアップでモビリティ MAC として使用する必要があります。柔軟性があり、カスタム MAC アドレスを設定することもできます。このアドレスは、`configure redundancy mobilitymac <custom mac address>` コマンドを使用してモビリティ MAC アドレスとして使用できます。設定した場合は、システム MAC アドレスの代わりにこの MAC アドレスを使用してモビリティ ピアを形成する必要があります。HA の設定後はこの MAC を変更できません。
- HA セットアップのサービス ポートには、DHCP アドレス割り当てを使用することをお勧めします。HA をイネーブルにした後でサービス ポートのスタティック IP を設定すると、WLC でサービス ポート IP が不明になり、再度設定する必要があります。
- SSO をイネーブルにした場合は、HA セットアップのいずれの WLC についても、サービス ポートでの SNMP と GUI のアクセスはありません。
- 仮想 IP アドレスの変更、セキュアな Web モードのイネーブル化、Web 認証プロキシの設定などの設定を実装するには、WLC のリブートが必要です。この場合は、アクティブ WLC のリブートによって、スタンバイ WLC の同時リブートもトリガーされます。
- アクティブ WLC で SSO をディセーブルにすると、これが、スタンバイ WLC にプッシュされます。リブート後は、すべてのポートがアクティブ WLC に表示され、スタンバイ WLC ではディセーブルになります。
- 優れたパフォーマンスを得るには、キープアライブと Peer Discovery のタイマーをデフォルト タイマー値のままにする必要があります。
- アクティブ WLC で設定をクリアすると、スタンバイ WLC での設定のクリアも開始されます。
- SSO をイネーブルにしてある場合、内部 DHCP はサポートされません。
- バージョン 7.5 およびそれ以降では、AP/クライアント SSO はアクティブとスタンバイ コントローラ間の L3 MGID の同期をサポートしています。
- LSC 証明書を備えた AP がサポートされています。SSO を有効化する前に、コントローラの LSC 証明書と SCEP の設定をアクティブ コントローラとスタンバイ コントローラで実施する必要があります。

注: スイッチ オーバー時のモビリティ ピアの動作は、アンカー コントローラとフォーリン コントローラで実行しているバージョンに依存します。アンカー コントローラとフォーリン コントローラの両方がバージョン 7.5 またはそれ以降を実行している場合、ローミング クライアントに影響はなく、ピアはスイッチオーバー メッセージを受け取り次第、AP リスト、回避リスト、インフラストラクチャ MFP キーを新しいアクティブ コントローラに送信します。
7.5 より前の HA をサポートするバージョン(7.3 および 7.4)を実行している WLC と 7.5 以降のバージョンを実行している WLC が混在しているモビリティ グループでは、スイッチ オーバーが発生すると、ローミング クライアントは、アンカーとフォーリン WLC の両方でクリーンアップされます。このため、HA ペアがモビリティ グループに存在する場合、そのモビリティ グループはイメージ バージョン 7.5 およびそれ以降を実行している WLC で構成することをお勧めします。WLC のモビリティ ピアのバージョンが 7.3 より前で HA をサポートしていない場合、この問題は存在しません。

メンテナンス モード

スタンバイ WLC がメンテナンス モードに入り、ネットワークおよびピアと通信できない複数のシナリオがあります。

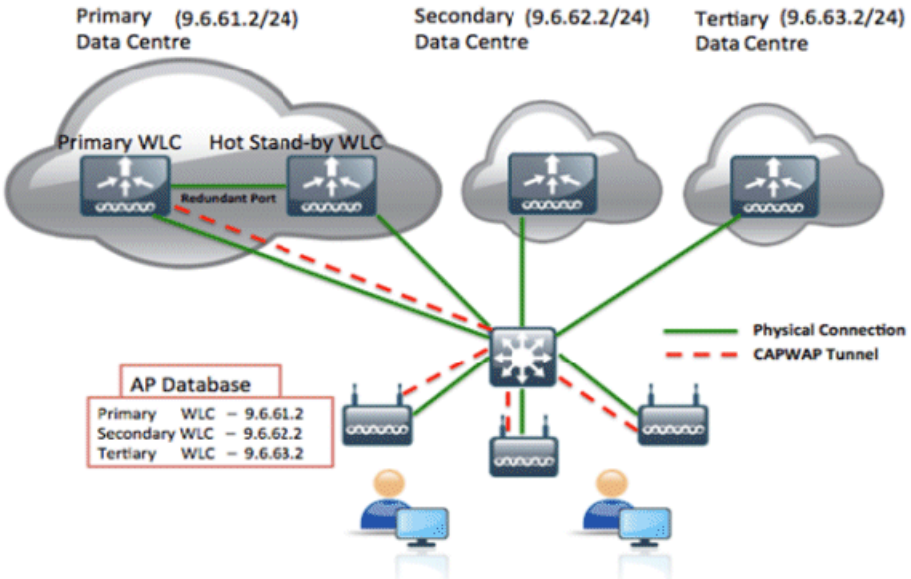
- 冗長管理インターフェイスを介してゲートウェイに到達できない
- HA SKU を持つ WLC がピアを検出しない
- 冗長ポートが停止している
- ソフトウェア バージョンの不一致(最初に起動する WLC がアクティブ モードになり、もう 1 つの WLC がメンテナンス モードになる)

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
      Local State = NEGOTIATION
       Peer State = DISABLED
             Unit = Secondary - HA SKU
          Unit ID = 00:24:97:69:78:20
Redundancy State = Non Redundant
    Mobility MAC = 00:24:97:69:D2:20

Maintenance Mode = Enabled
Maintenance cause= Negotiation Timeout

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

注: メンテナンス モードを終了するには、WLC をリブートする必要があります。メンテナンス モードでは、コンソールおよびサービス ポートのみがアクティブです。

レガシーのプライマリ、セカンダリ、ターシャリ HA と合わせた SSO 導入

HA(つまり AP SSO)は、現状同様に、セカンダリおよびターシャリのコントローラと組み合わせて導入できます。HA セットアップで組み合わされているアクティブとスタンバイの両方の WLC をプライマリ WLC として設定する必要があります。AP は、HA セットアップのアクティブとスタンバイの両方の WLC が故障したときに限り、セカンダリ、さらにはターシャリの WLC にフォールバックします。



モビリティ セットアップでの SSO 導入

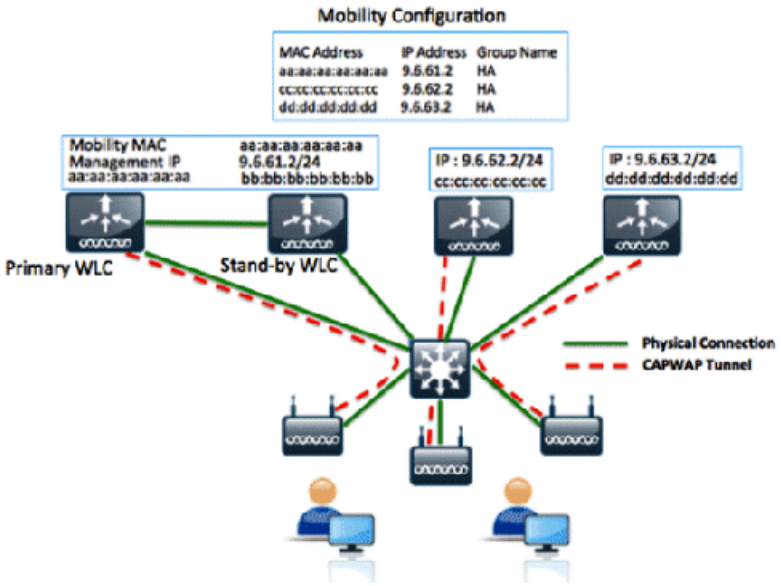
各 WLC は独自の一意の MAC アドレスを持ちます。このアドレスは、個々のコントローラ管理 IP アドレスと合わせてモビリティ設定で使用されます。HA(つまり AP SSO)セットアップでは、両方の WLC(プライマリおよびスタンバイ)が独自の一意の MAC アドレスを持ちます。プライマリ ボックスが故障し、スタンバイがネットワークを引き継ぐ場合に、プライマリ ボックスの MAC アドレスがモビリティ セットアップの別のコントローラで使用されていると、制御パスおよびデータ パスが切断され、ユーザは、モビリティ セットアップのすべてのコントローラでこの MAC をスタンバイ MAC アドレスに手動で変更する必要があります。手動による多数の介入を必要とするため、この処理は実に厄介です。

手動による介入なしにモビリティ ネットワークの安定性を保ち、故障またはスイッチオーバーに備えるために、交互(back-and-forth)モビリティ MAC 概念が導入されました。HA ペアを設定する場合、デフォルトでは、プライマリ WLC の MAC アドレスがモビリティ MAC アドレスとしてスタンバイ WLC で同期され、両方のコントローラで show redundancy summary コマンドによって参照できます。

```
(5508-Standby) >show redundancy summary
 Redundancy Mode = SSO ENABLED
            Unit = Secondary - HA SKU
         Unit ID = 00:24:97:69:78:20
Redundancy State = Non Redundant
    Mobility MAC = 00:24:97:69:D2:20

Redundancy Management IP Address.................. 9.6.61.23
Peer Redundancy Management IP Address............. 9.6.61.21
Redundancy Port IP Address........................ 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

スタンバイ コントローラでキャプチャされたこの出力ではモビリティ MAC アドレスを確認できます。これは、Unit ID として示されているスタンバイの MAC アドレスとは異なります。この MAC アドレスは、アクティブ WLC から同期されており、モビリティ設定で使用する必要があります。この実装では、アクティブ WLC が停止する場合、または交換する場合であっても、モビリティ MAC アドレスは引き続きスタンバイ WLC で使用可能で、アクティブです。前のアクティブ WLC を交換するために新しいコントローラをネットワークに導入する場合、このコントローラの状態はスタンバイに遷移し、同じモビリティ MAC アドレスが新しいスタンバイ WLC と再度同期されます。

この設定には柔軟性があり、アクティブ WLC の MAC アドレスをモビリティ MAC として使用するデフォルトの動作に代えて、カスタム MAC アドレスをモビリティ MAC として設定できます。これは、アクティブ WLC で configure redundancy mobilitymac <custom mac address> コマンドを使用して実施できます。設定後は、もう一方のコントローラでアクティブ WLC の MAC アドレスを使用する代わりにこの MAC アドレスを使用してモビリティ ピアを形成する必要があります。この MAC アドレスは、HA ペアを形成する前に設定する必要があります。HA ペアの形成後は、モビリティ MAC を変更、編集できません。



このトポロジでは、プライマリとスタンバイは、それぞれ独自の MAC アドレスを持ちます。HA ペアリングでは、アクティブ WLC の MAC アドレスがモビリティ MAC アドレスとして同期されます。これは、HA ペアリングの前にカスタム MAC が設定されていない場合のデフォルトの動作です。アクティブ WLC の MAC アドレスがモビリティ MAC アドレスとして同期された後は、モビリティ セットアップのすべてのコントローラのモビリティ設定で同じ MAC が使用されます。

HA ペアのライセンス

HA ペアは、次の組み合わせで稼働している 2 つの WLC 間に設定できます。

- 1 つの WLC に有効な AP カウント ライセンスがあり、もう 1 つの WLC に HA SKU UDI がある
- 両方の WLC に有効な AP カウント ライセンスがある
- 1 つの WLC に評価ライセンスがあり、もう 1 つの WLC に HA SKU UDI または永久ライセンスがある

1 つの WLC に有効な AP カウント ライセンスがあり、もう 1 つの WLC に HA SKU UDI がある

- HA SKU は AP カウント ライセンスがゼロの新しい SKU です。
- HA SKU を持つデバイスは、初めてペアになるときにスタンバイになります。
- AP カウント ライセンス情報は、アクティブからスタンバイにプッシュされます。
- アクティブが故障した場合、HA SKU では、取得した AP カウントを使用して AP が接続でき、90 日間のカウントダウンを開始します。このカウントダウンは、日単位です。
- 90 日間が経過すると、頻繁なメッセージの出力を開始します。接続されている AP を切断することはありません。
- 新しい WLC がアップすると、ペアリング時点の HA SKU が AP カウントを取得します。
  - 新しい WLC の AP カウントが前の WLC よりも大きい場合、90 日のカウンタはリセットされます。
  - 新しい WLC の AP カウントが前の WLC よりも小さい場合、90 日のカウンタはリセットされません。
  - スイッチオーバー後に AP カウントを下げるために、WLC オフセット タイマーが続行され、時間の経過後に頻繁なメッセージを表示します。
    - 経過時間および AP カウントは、リブート時に維持されます。
    - ファクトリ デフォルトの HA-SKU コントローラでは、AP の接続を許可してはいけません。

両方の WLC に有効な AP カウント ライセンスがある

- 最小永久ライセンス カウント要件を満たしているのであれば、CLI を使用して、1 つの WLC をスタンバイ WLC として設定する必要があります(設定のセクションを参照)。この条件は 5508 WLC だけに有効で、スタンバイに変換する最低 50 の AP 永久ライセンスが必要になります。5520、WiSM2、7500、および 8500 などの他の WLC に制約事項はありません。
- AP カウント ライセンス情報は、アクティブからスタンバイにプッシュされます。
- スイッチオーバーの場合、新しいアクティブ WLC は前のアクティブ WLC のライセンス カウントを使用して動作し、90 日のカウントダウンを開始します。
- セカンダリとして設定されている WLC は、インストールされている独自のライセンスを使用せず、アクティブから継承したライセンスのみを利用します。
- 90 日間が経過すると、頻繁なメッセージの出力を開始します。接続されている AP を切断することはありません。
- 新しい WLC がアップすると、ペアリング時点の HA SKU が AP カウントを取得します。
  - 新しい WLC の AP カウントが前の WLC よりも大きい場合、90 日のカウンタはリセットされます。
  - 新しい WLC の AP カウントが前の WLC よりも小さい場合、90 日のカウンタはリセットされません。
  - 小さい AP カウントへのスイッチオーバーの後も WLC オフセット タイマーは続行されて、時間の経過後に頻繁なメッセージを表示します。

1 つの WLC に評価ライセンスがあり、もう 1 つの WLC に HA SKU UDI または永久ライセンスがある

- HA SKU を持つデバイスは、評価ライセンスを実行している既存のアクティブ WLC と初めてペアになるときに、スタンバイ WLC になります。または、最小永久ライセンス カウント要件を満たしていれば、CLI 設定を使用して、永久ライセンス カウントを実行している任意の WLC をセカンダリ ユニットとして設定できます。この条件は 5508 WLC だけに有効で、スタンバイに変換する最低 50 の AP 永久ライセンスが必要になります。5520、WiSM2、7500、3504 および 8500 などの他の WLC に制約事項はありません。
- AP カウント ライセンス情報は、アクティブからスタンバイにプッシュされます。
- スイッチオーバーの場合、新しいアクティブ WLC は前のアクティブ WLC のライセンス カウントを使用して動作し、90 日のカウントダウンを開始します。
- 90 日間が経過すると、頻繁なメッセージの出力を開始します。接続されている AP を切断することはありません。
- 新しい WLC がアップすると、ペアリング時点の HA SKU が AP カウントを取得します。
  - 新しい WLC の AP カウントが前の WLC よりも大きい場合、90 日のカウンタはリセットされます。
  - 新しい WLC の AP カウントが前の WLC よりも小さい場合、90 日のカウンタはリセットされません。
  - 小さい AP カウントへのスイッチオーバーの後も WLC オフセット タイマーは続行されて、時間の経過後に頻繁なメッセージを表示します。

サポートされる HA トポロジ

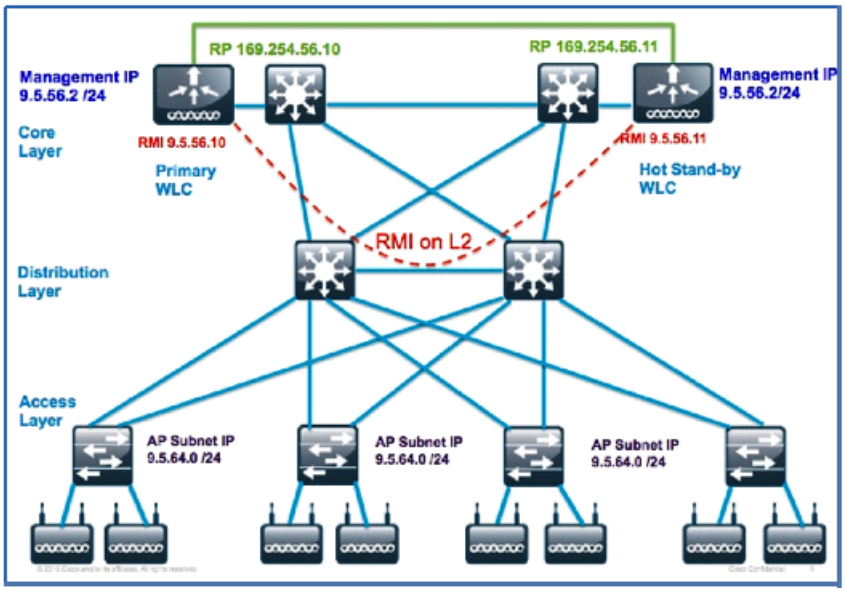
リリース 7.5 ～ 8.7 でサポートされる HA トポロジ

3500(リリース 8.5)/5500/7500/8500 シリーズ コントローラ

1. 2 つの WLC 間のバックツーバック冗長ポート(RP)接続、冗長性管理インターフェイス(RMI)接続でピアと管理ゲートウェイの到達可能性をチェック。
2. 2 つの WLC 間の L2 隣接の RP 接続、RMI 接続でピアと管理ゲートウェイの到達可能性をチェック。同じデータセンター内にある場合と、異なるデータセンターにある場合があります。
3. VSS ペアに接続された 2 台の 5508、7500 または 8500。プライマリ WLC が 1 台の 6500 に、スタンバイ WLC がもう 1 台の 6500 に接続。

バックツーバック RP 接続

図 1　バックツーバック RP 接続



- これは、コントローラのリリース 7.3 でサポートされたトポロジと同じです。
- 設定同期とキープアライブ メッセージは冗長ポートから送信されます。
- RMI インターフェイスは管理サブネットの一部として作成され、ピアと管理ゲートウェイの到達可能性を検査するために使用されます。
- RTT 遅延はデフォルトで 80 ミリ秒です。RTT は、100 ～ 400 ミリ秒の範囲で設定可能なキープアライブ タイマーの 80% にする必要があります。
- 障害検出時間は 3*100 + 60 + ジッター(12 ミリ秒)= ～ 400 ミリ秒

  注: 上記の等式で、3 はキープアライブ再試行回数、100 はキープアライブ タイマー、60 は 3*10 + 3*10(ピアへの 3 RMI ping + ゲートウェイへの 3 ping)です。
- 帯域幅:60 Mbps 以上
- MTU: 1500

プライマリ WLC の設定:

configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1

configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11

configure redundancy unit primary

configure redundancy mode sso

ホット スタンバイ WLC の設定:

configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1

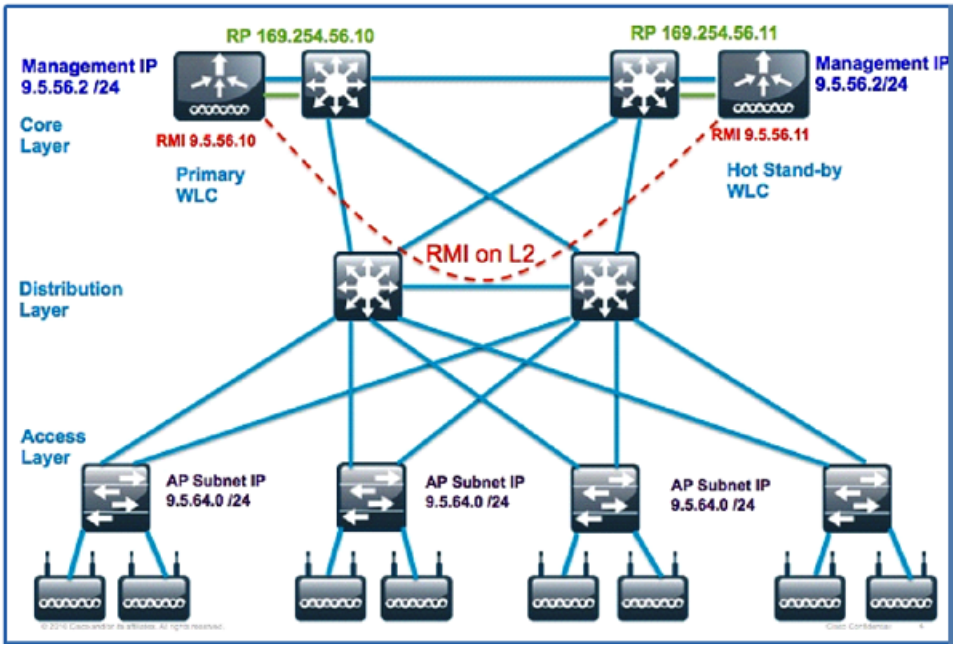
configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10

configure redundancy unit secondary

configure redundancy mode sso

スイッチを介した RP 接続

図 2　スイッチを介した RP 接続



- データセンターをまたぐ、スイッチを介した冗長ポート接続はこのトポロジでサポートされます。
- 設定同期およびキープアライブは冗長ポート経由。
- RMI インターフェイスは管理サブネットの一部として作成され、ピアと管理ゲートウェイの到達可能性を検査するために使用されます。
- RTT 遅延はデフォルトで 80 ミリ秒です。RTT は、100 ～ 400 ミリ秒の範囲で設定可能なキープアライブ タイマーの 80% にする必要があります。
- 障害検出時間は 3*100 + 60 + ジッター(12 ミリ秒)= ～ 400 ミリ秒
- 帯域幅:60 Mbps 以上
- MTU: 1500

プライマリ WLC の設定

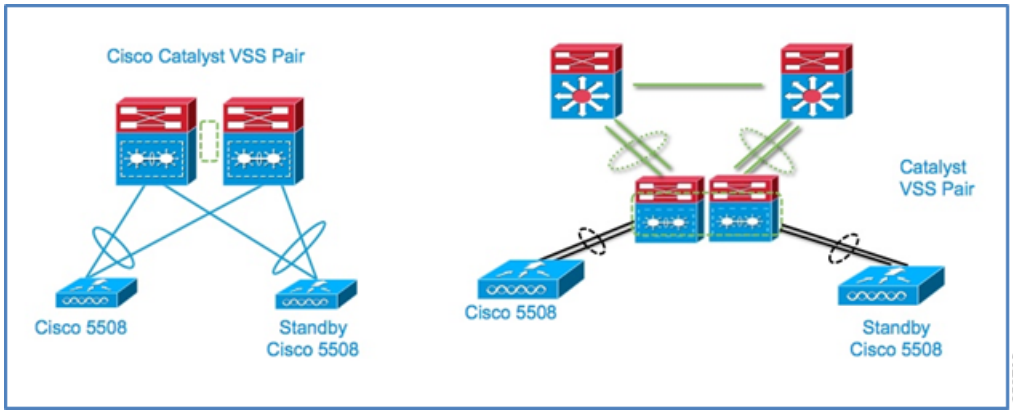
```
configure interface address management 9.5.56.2 255.255.255.0 9.5.56.1

configure interface address redundancy-management 9.5.56.10 peer-redundancy-management 9.5.56.11

configure redundancy unit primary

configure redundancy mode sso
```

ホット スタンバイ WLC の設定

```
configure interface address management 9.5.56.3 255.255.255.0 9.5.56.1

configure interface address redundancy-management 9.5.56.11 peer-redundancy-management 9.5.56.10

configure redundancy unit secondary

configure redundancy mode sso
```

VSS ペアに接続された 5508、7500 または 8500

図 3　VSS ペアに接続された WLC



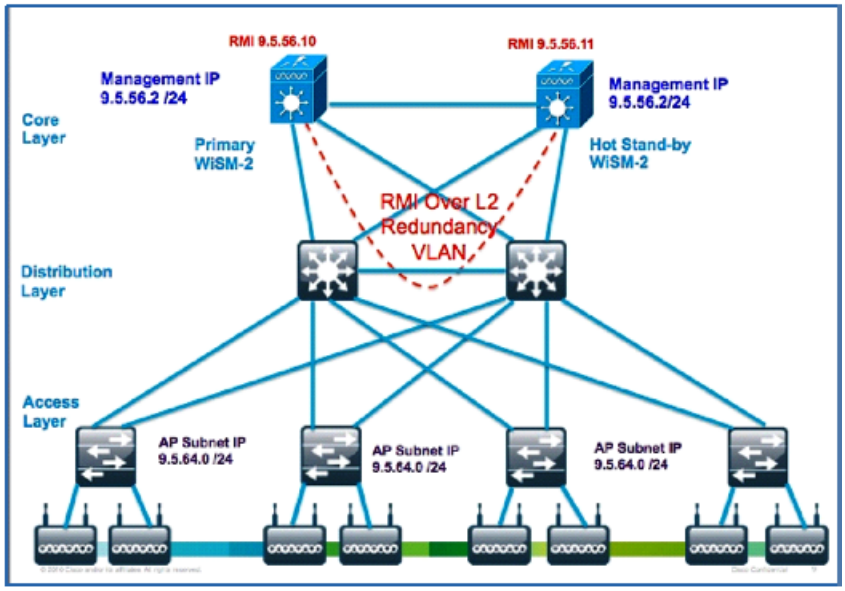
サポートされた WiSM2 コントローラの HA トポロジ

同一シャーシ内の WiSM2

図 4　単一シャーシ内の WiSM2

別のシャーシ内の WiSM2:L2 ネットワークによる冗長 VLAN

図 5　L2 ネットワークによる冗長 VLAN を使用した WiSM2 接続



Cat6k での WiSM2 用設定

wism service-vlan 192(サービス ポート VLAN)

wism redundancy-vlan 169(冗長ポート VLAN)

wism module 6 controller 1 allowed-vlan 24-38(データ VLAN)

WiSM2 HA 設定は変更されません。

別のシャーシ内の WiSM2:VSS ペア

図 6　VSS ペアを使用した WiSM2 接続

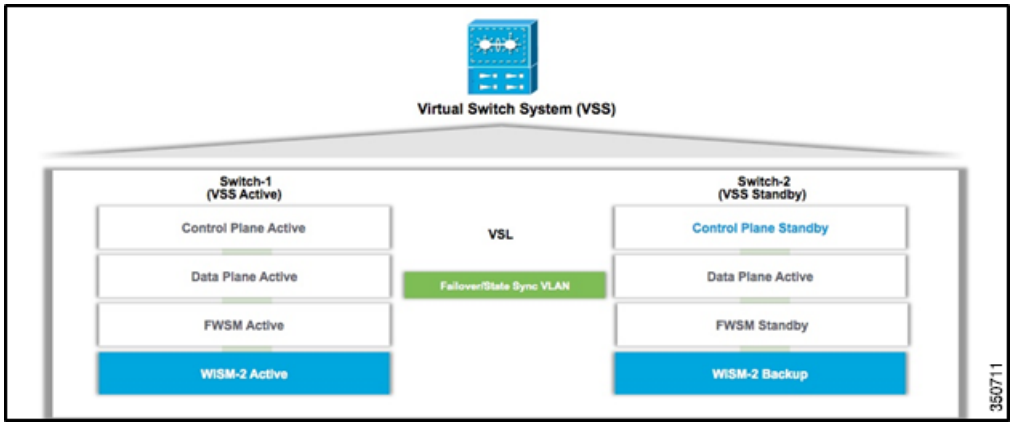


図 7　VSL リンクを介して接続されたアクティブおよびスタンバイ VSS ペア

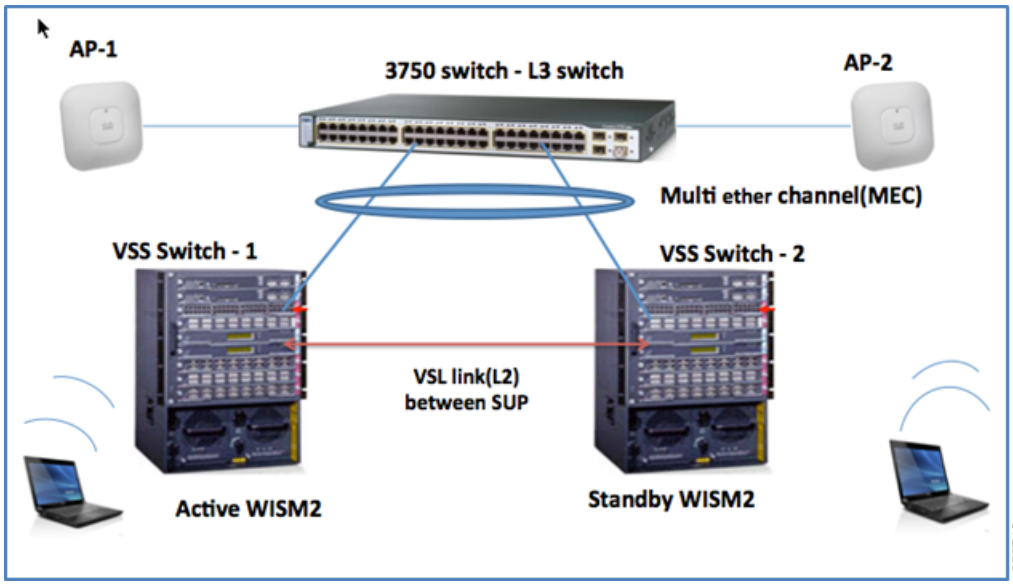
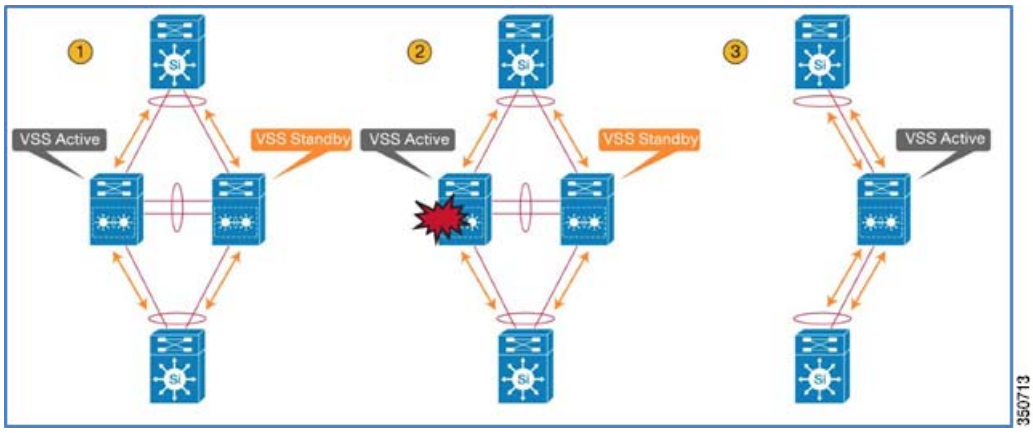


図 8　VSS ペアを使用した WiSM2 接続



VSS の設定

	Command	Purpose
Step 1	`Switch-1(config)#redundancy`	Enters redundancy configuration mode.
Step 2	`Switch-1(config-red)# mode sso`	Configures SSO. When this command is entered, the redundant supervisor engine is reloaded and begins to work in SSO mode.
Step 3	`Switch-1(config-red)# exit`	Exits redundancy configuration mode.
Step 4	`Switch-1(config)# router` *routing_protocol processID*	Enables routing, which places the router in router configuration mode.
Step 5	`Switch-1(config-router)#nsf`	Enables NSF operations for the routing protocol.
Step 6	`Switch-1(config-router)#end`	Exits to privileged EXEC mode.
Step 7	`Switch-1# show running-config`	Verifies that SSO and NSF are configured and enabled.
Step 8	`Switch-1# show redundancy states`	Displays the operating redundancy mode.

	Command	Purpose
Step 1	`Switch-1(config)# switch virtual domain 100`	Configures the virtual switch domain on Chassis A.
Step 2	`Switch-1(config-vs-domain)# switch 1`	Configures Chassis A as virtual switch number 1. For Chassis B config - Switch 2
Step 3	`Switch-1(config-vs-domain)# exit`	Exits config-vs-domain.

350714

Command	Purpose	
Step 1	`Switch-1(config)# interface port-channel 10`	Configures port channel 10 on Switch 1.
Step 2	`Switch-1(config-if)# switch virtual link 1`	Associates Switch 1 as owner of port channel 10.
Step 3	`Switch-1(config-if)# no shutdown`	Activates the port channel.
Step 4	`Switch-1(config-if)# exit`	Exits interface configuration.

	Command	Purpose
Step 1	`Switch-2(config)# interface port-channel 20`	Configures port channel 20 on Switch 2.
Step 2	`Switch-2(config-if)# switch virtual link 2`	Associates Switch 2 as owner of port channel 20.
Step 3	`Switch-2(config-if)# no shutdown`	Activates the port channel.
Step 4	`Switch-2(config-if)# exit`	Exits interface configuration mode.

Command	Purpose
`Switch-1# switch convert mode virtual`	Converts Switch 1 to virtual switch mode. After you enter the command, you are prompted to confirm the action. Enter**yes**. The system creates a converted configuration file, and saves the file to the RP bootflash.

350715

推奨事項

- 冗長リンクのラウンドトリップ遅延は、80 ミリ秒以下にする必要があります。
- 冗長リンクの推奨 MTU は 1500 以上です。
- 冗長リンクの帯域幅は 60 Mbps 以上である必要があります。
- 2 台のコントローラ間に L2 隣接があるといった、冗長ポートがスイッチを介して接続されている場合、RP VLAN は管理ポートのスイッチに設定されたアクセス VLAN から除外する必要があります。
- L2 ネットワーク経由で接続される 2 種類のシャーシ間の WiSM2 接続の場合、「redundancy vlan」が管理ポートのスイッチに設定されたアクセス VLAN から除外される必要があります。
- アクティブ-アクティブ シナリオを回避するため、RP ポート接続と管理ポートのトラフィックに、異なるスイッチ セットを使用することを強く推奨します。
- VSS セットアップの WiSM2 を配置する場合、ピア検出時間を 180 秒に設定することを推奨します。

AP とクライアントの状態の同期

1. この段階では、両方のコントローラが HA セットアップでペアになります。アクティブで実施した設定はすべて、冗長ポート経由でスタンバイ コントローラに同期されます。コンソール接続から、スタンバイ WLC の WLAN サマリーとインターフェイス サマリーを確認します。
2. ハイ アベイラビリティのセットアップでは、UP Time や Association UP time など、アクティブ コントローラおよびスタンバイ コントローラ(Run 状態の AP のみ)に維持されている AP の CAPWAP の状態が、アクティブ コントローラからスタンバイ コントローラに同期されます。以下の例では、WLC 1 がアクティブ状態でネットワークを処理しており、WLC 2 がスタンバイ状態でアクティブ コントローラをモニタしています。WLC 2 はスタンバイ状態ですが、まだ AP の CAPWAP 状態を維持します。

   WLC 1-> コンソール接続:

```
(POD1-WLC) >show ap uptime

Number of APs.................................... 2
Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time              Association Up Time
-----------------   ----------------   ---------------------   ---------------------
POD1-AP1            6c:20:56:e1:50:09  0 days, 03 h 45 m 58 s  0 days, 00 h 24 m 11 s
POD1-AP2            44:d3:ca:42:31:57  0 days, 15 h 46 m 37 s  0 days, 00 h 24 m 07 s
```

350687

   アクティブ WLC の AP UP Time および Association UP Time を監視します

   WLC 2-> コンソール接続:

```
(POD1-WLC-Standby) >show ap uptime

Number of APs.................................... 2
Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time              Association Up Time
-----------------   ----------------   ---------------------   ---------------------
POD1-AP1            6c:20:56:e1:50:09  0 days, 03 h 46 m 11 s  0 days, 00 h 24 m 24 s
POD1-AP2            44:d3:ca:42:31:57  0 days, 15 h 46 m 50 s  0 days, 00 h 24 m 20 s
```

350688

   スタンバイ WLC の AP Up Time および Association UP Time がアクティブ WLC と同期するのを監視します。

3. ボックス フェールオーバー(アクティブ コントローラのクラッシュ/システム ハング/手動リセット/強制スイッチオーバー)の場合、ネットワークの引き継ぎのため、ダイレクト コマンドが冗長管理インターフェイスからスタンバイ コントローラに送られ、冗長ポート経由でアクティブ コントローラからも送られます。フェールオーバーは、アクティブ コントローラの AP/クライアントの数によって 2 ～ 360 ミリ秒かかります。アクティブ WLC に電源障害またはスイッチオーバーのダイレクト コマンドをスタンバイ コントローラに送信できない何らかのクラッシュが発生した場合は、360 ～ 990 ミリ秒かかり、アクティブ コントローラの AP/クライアントの数および設定されたキープアライブ タイマーによって変わります。デフォルトのキープアライブ タイマーは 100 ミリ秒です。デフォルト RTT 遅延が 80 ミリ秒以下であることを確認します。

4. クライアント SSO の一部として、リリース 7.5 では、クライアント データベースもスタンバイ WLC に同期され、スタンバイ WLC には Run 状態のクライアント エントリが出現します。

   WLC 1-> コンソール/Telnet/SSH 接続:

```
(POD1-WLC) >show client summary

Number of Clients.............................. 2

Number of PMIPV6 Clients....................... 0

                                                GLAN/
                                                RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol         Port Wired PMIPV6 Role
----------------- ----------------- ---- ------------ ----- ---- ---------------- ---- ----- ------ ----------------
24:77:03:11:59:38 POD1-AP1          1    Associated    1     Yes  802.11n(5 GHz)   1    No    No     Local
28:e7:cf:ec:e9:50 POD1-AP2          1    Associated    2     Yes  802.11n(5 GHz)   1    No    No     Local
```

350689

```
(POD1-WLC) >show client detail 28:e7:cf:ec:e9:50
Client MAC Address............................... 28:e7:cf:ec:e9:50
Client Username ................................. N/A
AP MAC Address................................... 64:d9:89:42:34:70
AP Name.......................................... POD1-AP2
AP radio slot Id................................. 1
Client State..................................... Associated
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 2
Hotspot (802.11u)................................ Not Supported
BSSID............................................ 64:d9:89:42:34:7e
Connected For ................................... 252 secs
Channel.......................................... 149
IP Address....................................... 10.10.11.76
Gateway Address.................................. 10.10.11.1
Netmask.......................................... 255.255.255.0
IPv6 Address..................................... fe80::2ae7:cfff:feec:e950
Association Id................................... 1
Authentication Algorithm......................... Open System
Reason Code...................................... 1
Status Code...................................... 0
Session Timeout.................................. 1800
Client CCX version............................... No CCX support
```

350690

   クライアント エントリはアクティブ WLC に存在します。

WLC 2-> コンソール接続:

```
(POD1-WLC-Standby) >show client summary

Number of Clients.............................. 2

Number of PMIPV6 Clients....................... 0

                                          GLAN/
                                          RLAN/
MAC Address       AP Name          Slot Status       WLAN  Auth Protocol        Port Wired PMIPV6 Role
----------------- ---------------- ---- ------------ ----- ---- --------------- ---- ----- ------ ----------
24:77:03:11:59:38 POD1-AP1          1   Associated    1    Yes  802.11n(5 GHz)  1    No    No     Local
28:e7:cf:ec:e9:50 POD1-AP2          1   Associated    2    Yes  802.11n(5 GHz)  1    No    No     Local
```

350691

```
(POD1-WLC-Standby) >show client detail 28:e7:cf:ec:e9:50
Client MAC Address.............................. 28:e7:cf:ec:e9:50
Client Username ................................ N/A
AP MAC Address.................................. 64:d9:89:42:34:70
AP Name......................................... POD1-AP2
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 2
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 64:d9:89:42:34:7e
Connected For .................................. 262 secs
Channel......................................... 149
IP Address...................................... 10.10.11.76
Gateway Address................................. 10.10.11.1
Netmask......................................... 255.255.255.0
IPv6 Address.................................... fe80::2ae7:cfff:feec:e950
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
```

350692

クライアント エントリはスタンバイ WLC に存在します。

5. PMK キャッシュも 2 台のコントローラ間で同期されます。

WLC 1:

```
(POD1-WLC) >show pmk-cache all

Number of PMK Cache Entries: 2

PMK-CCKM Cache
                          Entry
Type       Station        Lifetime   VLAN Override       IP Override         Audit-Session-ID
------   ---------------  --------   -----------------   ----------------    ----------------
RSN    28:e7:cf:ec:e9:50   83725                          0.0.0.0
RSN    70:de:e2:0e:ce:05   83725                          0.0.0.0
```

WLC 2:

```
(POD1-WLC-Standby) >show pmk-cache all
Number of PMK Cache Entries: 2

PMK-CCKM Cache

                          Entry
Type       Station        Lifetime   VLAN Override       IP Override          Audit-Session-ID
------     -------------  --------   -----------------   ---------------      ----------------
RSN    28:e7:cf:ec:e9:50  83725                           0.0.0.0
RSN    70:de:e2:0e:ce:05  83725                           0.0.0.0
```

350694

フェールオーバー プロセス

1. アクティブ コントローラで **redundancy force-switchover** コマンドを発行します。このコマンドを発行すると、アクティブ コントローラがリブートしてスタンバイ コントローラがネットワークを引き継ぐ手動スイッチオーバーがトリガーされます。この場合、アクティブ WLC の Run 状態のクライアントは、認証解除されません。コマンド **save config** が **redundancy force-switchover** コマンドの前に発行されます。

   WLC 1-> コンソール接続:

```
(POD1-WLC) >redundancy force-switchover

Warning: Saving configuration change causes all the configurations to be saved on flash.
If this is not what you intend to do, do not type 'y' below.

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!Restarting system.
```

350695

   WLC 2-> コンソール接続:

```
(POD1-WLC-Standby) >
HA completed successfully, WLC switch over detection time : 2 msec and APs switch over time : 0 msec

(POD1-WLC) >show client detail 28:e7:cf:ec:e9:50
Client MAC Address.............................. 28:e7:cf:ec:e9:50
Client Username ................................ N/A
AP MAC Address.................................. 64:d9:89:42:34:70
AP Name......................................... POD1-AP2
AP radio slot Id................................ 1
Client State.................................... Associated
Client NAC OOB State............................ Access
Wireless LAN Id................................. 2
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 64:d9:89:42:34:7e
Connected For .................................. 284 secs
Channel......................................... 149
IP Address...................................... 10.10.11.76
Gateway Address................................. 10.10.11.1
Netmask......................................... 255.255.255.0
IPv6 Address.................................... fe80::2ae7:cfff:feec:e950
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
```

350696

   上の画面キャプチャのプロンプトで変化を監視します。

WLC 2-> コンソール接続:

```
(POD1-WLC) >show ap uptime

Number of APs.................................... 2
Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Ethernet MAC       AP Up Time                 Association Up Time
------------------  -----------------  -------------------------  -------------------------
POD1-AP1            6c:20:56:e1:50:89  0 days, 03 h 57 m 13 s     0 days, 00 h 35 m 26 s
POD1-AP2            44:d3:ca:42:31:57  0 days, 15 h 57 m 52 s     0 days, 00 h 35 m 22 s
```

350697

当初はスタンバイでスイッチオーバー後にアクティブになった WLC 2 で AP CAPWAP State を監視します。AP Up Time および Association Up Time は維持され、AP は Discovery 状態になりませんでした。

2. また、スイッチオーバーが開始されるときのクライアント接続にも注意します。クライアントは、認証解除されません。

スイッチオーバー中の無線クライアントからゲートウェイ IP アドレスと管理 IP アドレスへの ping は、最小の損失を示します。

```
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=139ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time=55ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127
Reply from 10.10.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.2:
    Packets: Sent = 63, Received = 63, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 139ms, Average = 3ms
```

350698

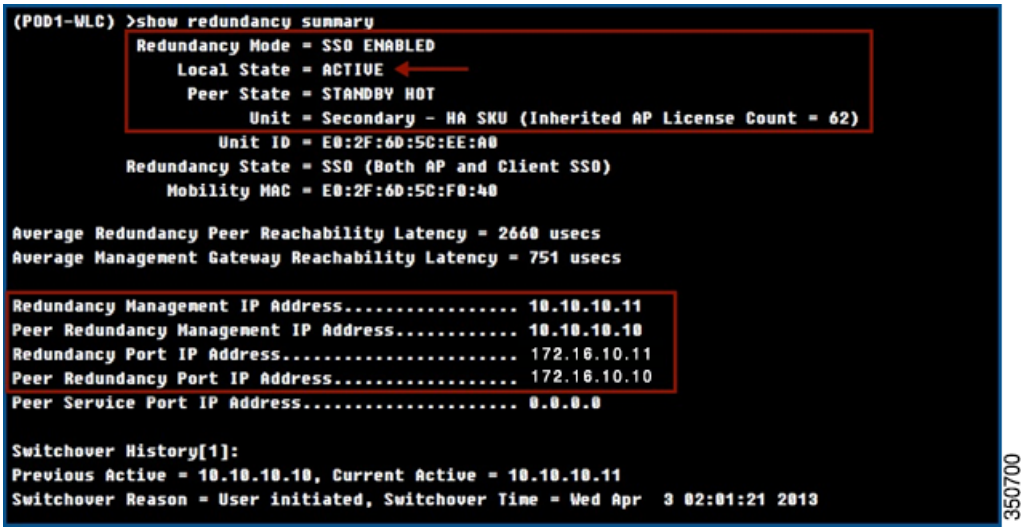
```
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=3ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=2ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255
Reply from 10.10.10.1: bytes=32 time=3ms TTL=255
Reply from 10.10.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.10.1:
    Packets: Sent = 49, Received = 49, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 0ms
```

350699

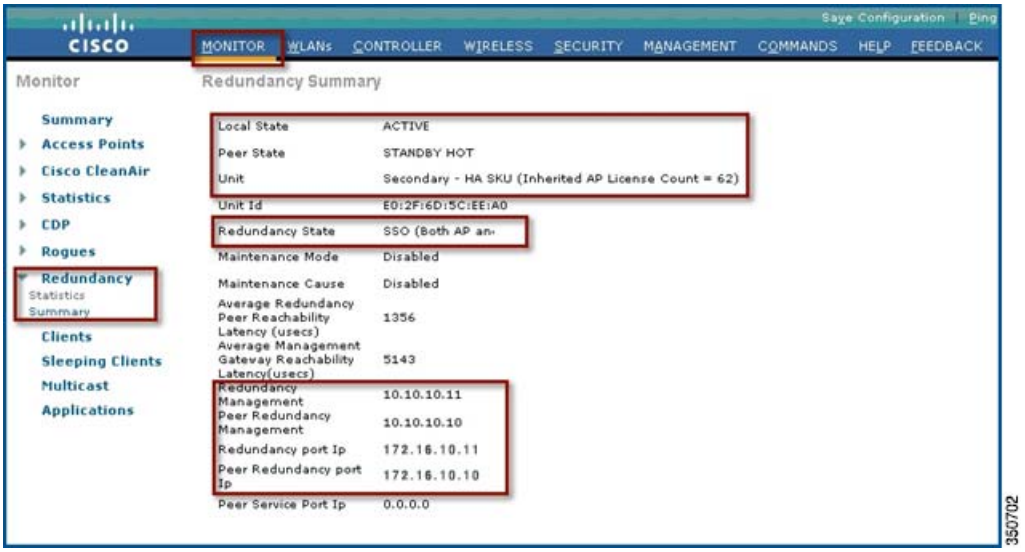
3. 冗長性ステータスのチェック方法

   WLC 1 -> コンソール接続でコマンド **show redundancy summary** を発行:

   WLC 2 -> コンソール接続でコマンド **show redundancy summary** を発行:



   WLC 2 -> [Monitor] > [Redundancy] > [Summary] とクリック:



4. 現在のアクティブ WLC への強制的な再スイッチオーバーを開始します。

   プライマリ ユニットとして設定された WLC がアクティブになり、セカンダリ ユニットとして設定された WLC 2 はホット スタンバイ状態になる必要があります。

WLC 2:

```
(POD1-WLC) >redundancy force-switchover

Warning: Saving configuration change causes all the configurations to be saved on Flash.
If this is not what you intend to do, do not type 'y' below.

The system has unsaved changes.
Would you like to save them now? (y/N) y


Configuration Saved!Restarting system.
```

350703

WLC 1:スイッチオーバー後に WLC 1 のローカル状態がアクティブ、ユニットがプライマリになっていることを確認します。

```
(POD1-WLC) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                Peer State = STANDBY HOT
                      Unit = Primary
                   Unit ID = E0:2F:6D:5C:F0:40
          Redundancy State = SSO (Both AP and Client SSO)
              Mobility MAC = E0:2F:6D:5C:F0:40
Management Gateway Failover = ENABLED (Management GW failover would be operational in few moments)
           Link Encryption = DISABLED

Redundancy Management IP Address.............. 10.10.10.10
Peer Redundancy Management IP Address........... 10.10.10.11
Redundancy Port IP Address..................... 169.254.10.10
Peer Redundancy Port IP Address................ 169.254.10.11
Peer Service Port IP Address................... 0.0.0.0
```

スイッチオーバー履歴を監視します。WLC は、10 回のスイッチオーバー履歴を原因とともに保持します。

```
Switchover History[1]:
Previous Active = 10.10.10.10, Current Active = 10.10.10.11
Switchover Reason = User initiated, Switchover Time = Wed Apr  3 02:01:21 2013
```

350705

クライアント SSO の動作と制限

- サービスおよびサービスに関連付けられたサービス プロバイダーおよびドメイン名データベースからなる Bonjour ダイナミック データベースがスタンバイに同期されます。
- Run 状態にあるクライアントだけが、アクティブとスタンバイの WLC 間で同期されます。クライアント SSO は、コントローラの関連付け/join プロセス中にあるクライアントのシームレスな遷移をサポートしません。遷移段階のクライアントはスイッチオーバーの後に認証解除され、コントローラに再度 join する必要があります。
- クライアントが Run 状態にない場合、ポスチャおよび NAC OOB はサポートされません。
- リリース 8.2.111.0 では、WGB および WGB に関連付けられているクライアントは、クライアント SSO によりステートフルでスイッチオーバーします。
- CCX ベース アプリケーションは、スイッチオーバー後に再度開始する必要があります。
- 新しいモビリティはサポートされていません。
- クライアントの統計情報は同期されません。

- PMIPv6、NBAR、SIP スタティック CAC ツリーは同期されず、SSO 後に再学習する必要があります。
- OEAP(600)クライアントはサポートされません。
- パッシブ クライアントは SSO 後に再度関連付ける必要があります。
- デバイスとルート証明書はスタンバイ コントローラに自動同期されません。
- AP およびクライアントの不正情報はスタンバイ コントローラに同期されず、ホット スタンバイがアクティブ コントローラになったときに再学習が必要です。
- スリープ状態のクライアント情報は、スタンバイ コントローラに同期されません。
- NBAR 統計情報はセカンダリ コントローラに同期されません。
- ネイティブ プロファイリング データはセカンダリ コントローラに同期されないため、クライアントはスイッチオーバー後に再度プロファイリングされます。
- 次の表は、MAP と RAP での w.r.t SSO の動作を示します。

	AP SSO	クライアント SSO
RAP	サポートあり	サポート対象外
Map	未サポート	サポート対象外

リリース 8.0 のハイ アベイラビリティ

リリース 8.0 では、ハイ アベイラビリティ機能セットが強化および改善されています。このセクションでは次の機能強化について取り上げます。

- Bulk Sync ステータス
- HA で強化されたデバッグと有用性
- 設定可能なキープアライブ タイマー/リトライとピア検索タイマー値
- Peer RMI ICMP ping を UDP メッセージに変更
- スタンバイ WLC のオンザフライのメンテナンス モード
- デフォルト ゲートウェイの到達可能性のチェック機能の強化
- 高速 HA ペア設定

リリース 8.0 のハイ アベイラビリティでは、SSO を有効にする次のような新機能も導入されています。

- 内部 DHCP サーバによる SSO 対応コントローラのサポート
- AP 無線の CAC 統計情報の同期
- スリープ状態のクライアント機能の SSO サポート
- OEAP 600 AP の SSO サポート

注: リリース 8.0 以降では、不正なスイッチオーバーを避けるために、RMI および管理インターフェイスを必ずタグ付けする必要があります。

機能強化と改善

Bulk Sync ステータス

現在コントローラは、Bulk Sync 設定が開始されても、その完了を示すものを何も提供しません。Bulk Sync を確認する手段は、ユーザによる監視とスタンバイ WLC に同期されたクライアントの数を手動でチェックする方法のみです。この機能の一部として、スタンバイ WLC の起動時に Bulk Sync のステータス(AP とクライアント同期の両方)を伝えるためのメカニズムが提供されています。

[Controller] > [Redundancy] > [Summary] の下に、[BulkSync Status] と呼ばれる新しいフィールドが GUI として追加されています。このフィールドは、スタンバイ WLC への一括同期のステータスを示し、ステータスは Pending/In-progress/Complete のいずれかになります。

図 9　BulkSync Status GUI

また、CLI コマンド **`show redundancy summary`** の出力にも、スタンバイ コントローラとのペアリング中は Bulk Sync ステータスが表示されます。ステータスは、以下に示すように Pending/In-progress/Complete のいずれかになります。

スタンバイ コントローラの起動中、**BulkSync** ステータスには [Pending] と表示されます。

図 10 BulkSync Status:Pending

```
(Cisco Controller) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = UNKNOWN - Communication Down
                       Unit = Primary
                    Unit ID = 6C:20:56:64:B9:A0
          Redundancy State = Non Redundant
              Mobility MAC = 6C:20:56:64:B9:A0
            BulkSync Status = Pending
```

352777

スタンバイ コントローラがブートアップ プロセスを完了し、一括同期が開始されると、ステータスは [In-Progress] に変わります。

図 11 BulkSync Status:In-Progress

```
(Cisco Controller) >
Blocked: Configurations blocked as standby WLC is still booting up.
         You will be notified once configurations are Unblocked

Unblocked: Configurations are allowed now...

(Cisco Controller) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = STANDBY HOT
                       Unit = Primary
                    Unit ID = 6C:20:56:64:B9:A0
          Redundancy State = SSO
              Mobility MAC = 6C:20:56:64:B9:A0
            BulkSync Status = In-Progress
Average Redundancy Peer Reachability Latency = 0 usecs
Average Management Gateway Reachability Latency = 5802 usecs
```

一括同期プロセスが完了すると、**BulkSync** ステータスは [Complete] に変わります。

図 12 BulkSync Status:Complete

```
(Cisco Controller) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = STANDBY HOT
                       Unit = Primary
                    Unit ID = 6C:20:56:64:B9:A0
          Redundancy State = SSO
              Mobility MAC = 6C:20:56:64:B9:A0
            BulkSync Status = Complete
Average Redundancy Peer Reachability Latency = 459 usecs
Average Management Gateway Reachability Latency = 4520 usecs
```

debug/show コマンドの機能強化

HA はネットワークが停止しないようにする上で重要な役割を果たすため、SSO の時点で、またはそれ以降の時点で、ボックスの状態の変化をデバッグできるかどうかにも直接かかわります。

次の新しいカテゴリの統計情報が [Monitor] > [Redundancy] > [Statistics] の下に表示されるようになりました。

a. All

b. Infra

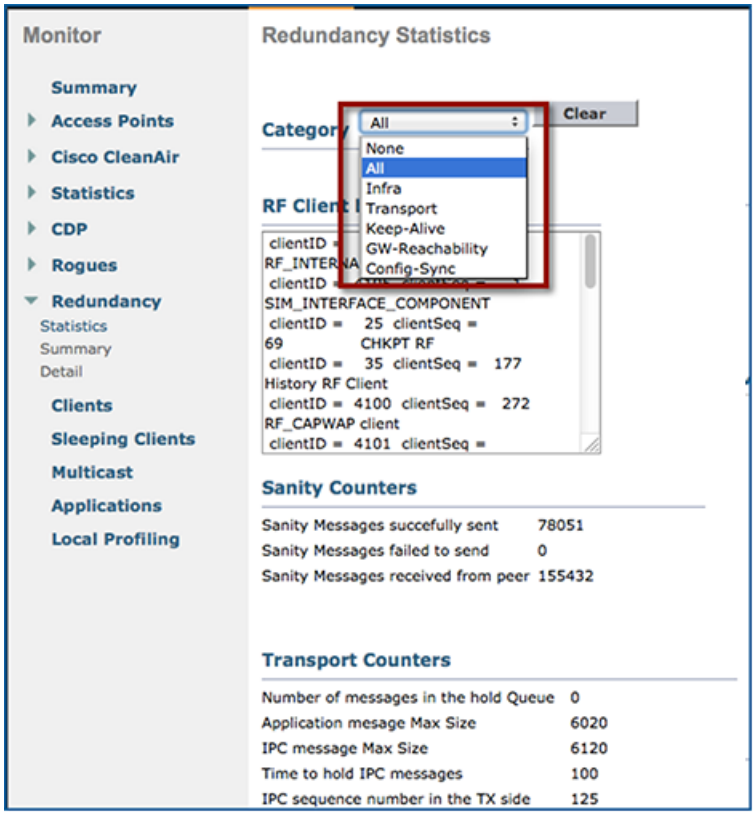
c. Transport

d. Keep-Alive

e. GW-Reachability

f. Config-Sync

図 13 Redundancy Statistics の GUI



Infra 統計情報には、図 14(57 ページ)に示すように RF クライアントの詳細情報とサニティ カウンタが表示されます。

図 14 Redundancy Statistics:Infra

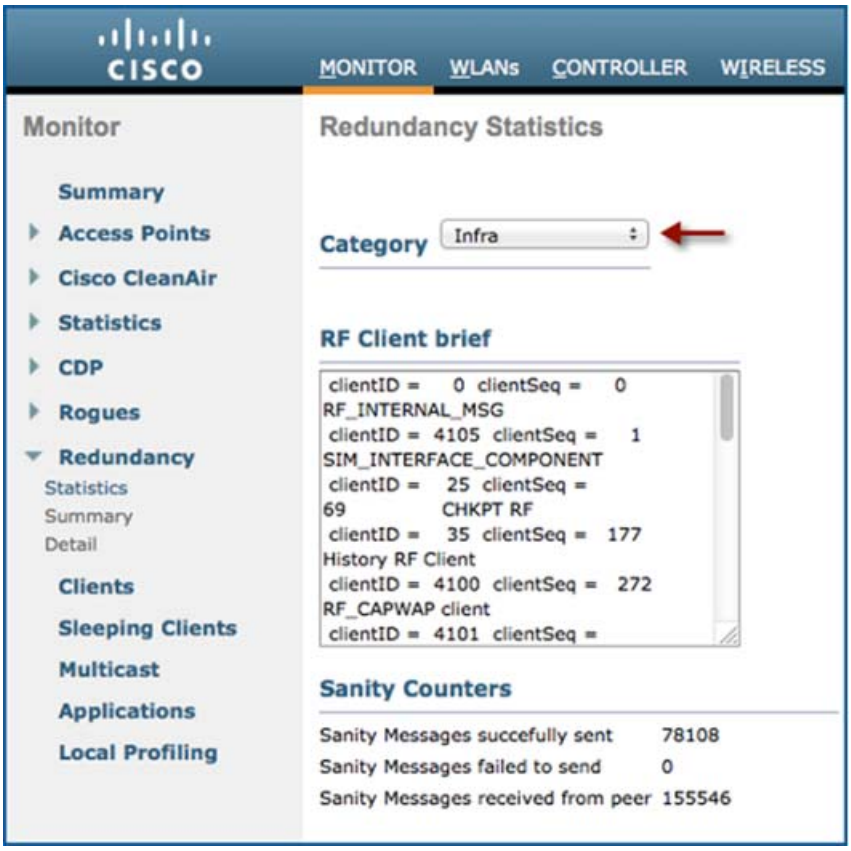
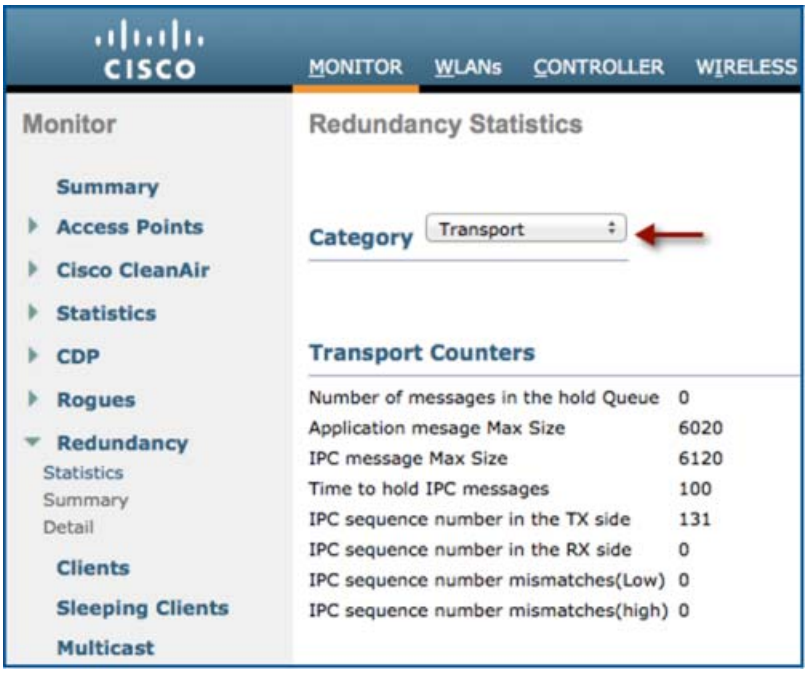
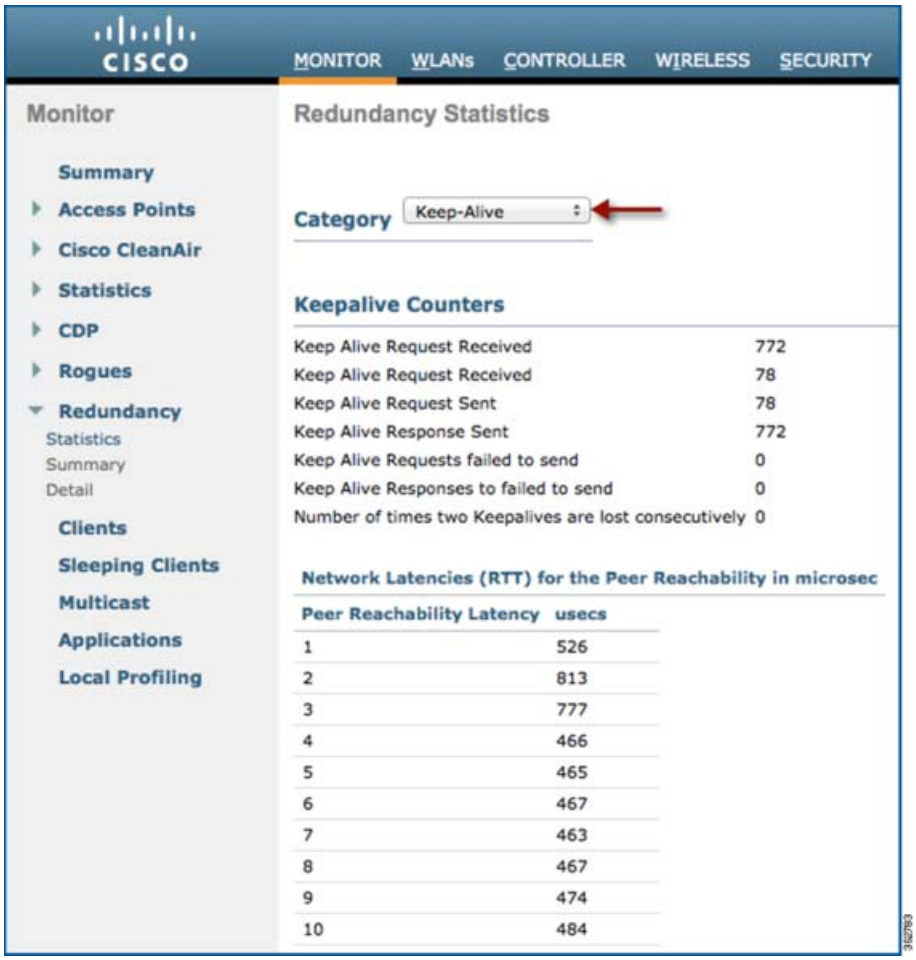


図 15 Redundancy Statistics:Transport



ハートビート デバッグには、ハートビートの受信イベント、ハートビートの損失イベント、およびそれらに関連した後続のアクションが含まれます。

図 16 Redundancy Statistics:Keep-Alive



HA システムは、ネットワークの停止を削減するために、管理ゲートウェイの到達可能性を監視します。

スタンバイ コントローラでは、アクティブ コントローラとスタンバイ コントローラのゲートウェイの到達可能性に関連する有用性のデバッグ、それぞれの稼働状態、およびこの情報に基づいて行われたアクションが報告されます。アクティブ コントローラでは、アクティブ WLC のゲートウェイへの到達可能性のみが報告されます。

図 17 Redundancy Statistics:GW-Reachability

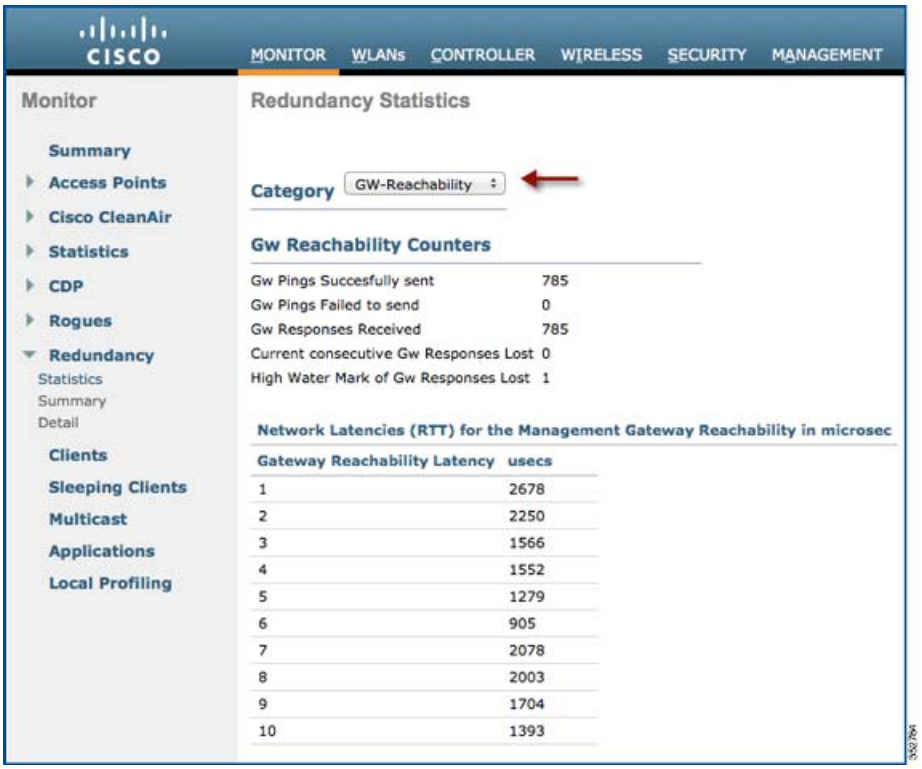
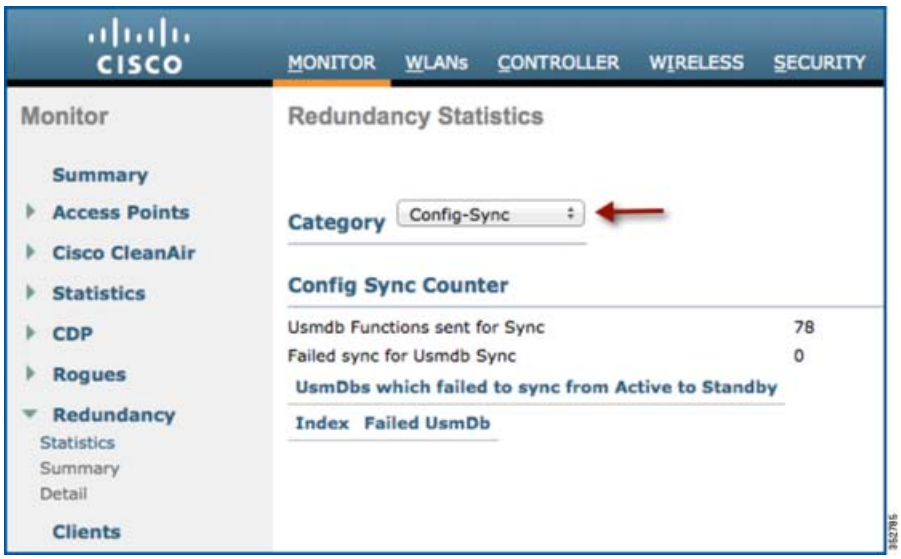


図 18 Redundancy Statistics:Config-Sync



この機能のために、次の debug/show CLI コマンドが導入されています。

1. **debug redundancy infra detail/errors/event**
2. **debug redundancy transport detail/errors/events/packet**
3. **debug redundancy keepalive detail/errors/events**
4. **debug redundancy gw-reachability detail/errors/events**
5. **debug redundancy config-sync errors/events/detail**
6. **debug redundancy ap-sync errors/events/detail**
7. **debug redundancy client-sync errors/events/detail**
8. **debug redundancy mobility events/errors/detail**
9. **show redundancy infra statistics**
10. **show redundancy transport statistics**
11. **show redundancy keepalive statistics**
12. **show redundancy gw-reachability statistics**
13. **show redundancy config-sync statistics**
14. **show redundancy ap-sync statistics**
15. **show redundancy client-sync statistics**

設定可能なキープアライブとピア検索のパラメータ

顧客の導入状況ごとに異なるネットワークの遅延に対処するため、キープアライブ パラメータとピア検索パラメータが設定可能になりました。この機能強化により、アクティブ コントローラとスタンバイ コントローラ間のフェールオーバーをトリガーするキープアライブの最大数を設定できるようになりました。また、ピア検索タイマーとキープアライブ タイマーも広い範囲をサポートするように変更されています。

次の新しい CLI コマンドが追加されており、3 ～ 10 の範囲で冗長キープアライブ リトライの回数を設定できます。

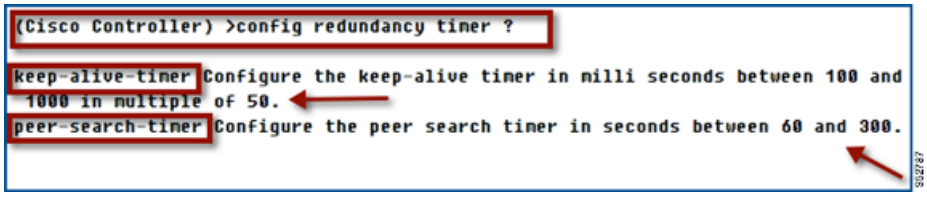
図 19 redundancy retries CLI コマンド

```
(Cisco Controller) >config redundancy retries ?

keep-alive-retry Configure the keep-alive retry count between 3 and 10
gateway-retry  Configure the gateway retry count values between 6 to 12

(Cisco Controller) >config redundancy retries keep-alive-retry ?

<retry count>  Configures keep-alive retry count between 3 and 10
```

キープアライブ タイマーの既存の CLI コマンド **config redundancy timer keep-alive-timer** が 100 ～ 1000 ミリ秒のキープアライブ タイマーをサポートするように変更されています。

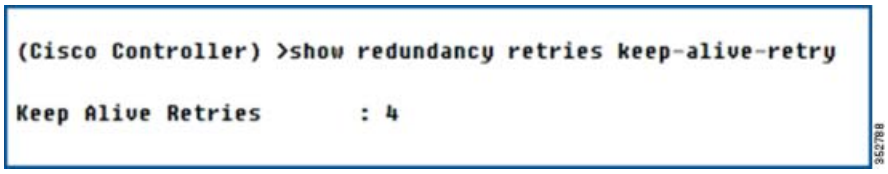
ピア検索タイマーの既存の CLI コマンド **config redundancy timer peer-search-timer** が 60 ～ 300 秒のピア検索タイマーをサポートするように変更されています。

図 20 redundancy timer CLI コマンド



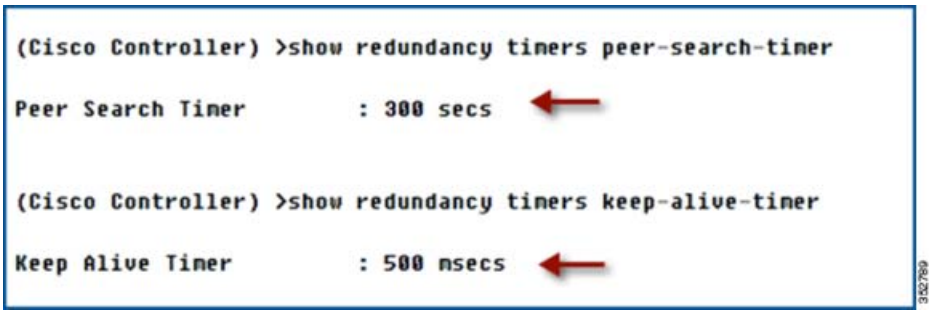
冗長キープアライブ リトライ値を表示するために、次の CLI が導入されています。

図 21 show redundancy retries CLI コマンド



ピア検索タイマーおよびキープアライブタイマー値を表示するには、**show redundancy timers** コマンドを使用します。

図 22 Show redundancy timers CLI コマンド



キープアライブ値とピア検索タイムアウト値を表示するには、**show redundancy detail** コマンドを使用します。

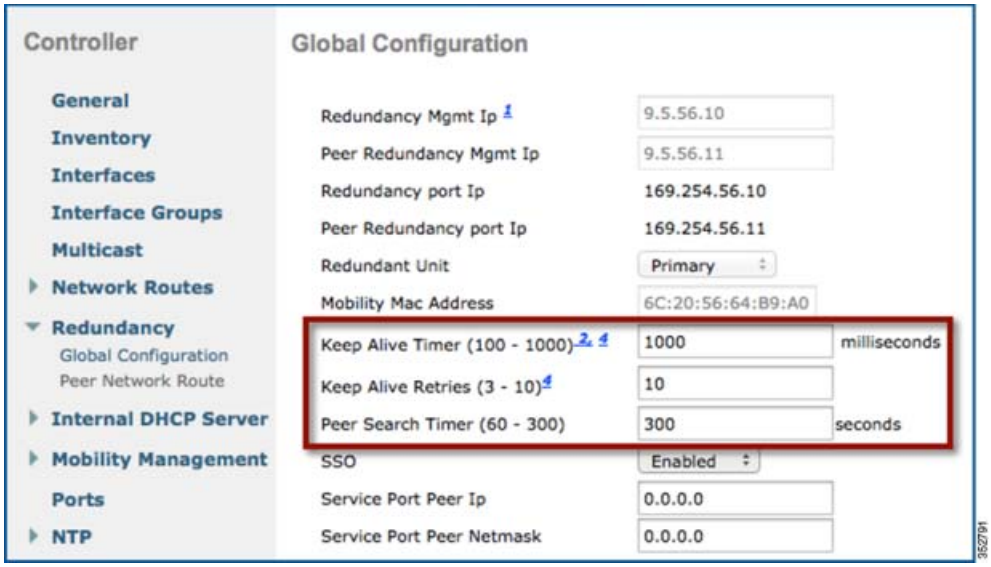
図 23 `Show redundancy detail` CLI コマンド

```
(Cisco Controller) >show redundancy detail ?

(Cisco Controller) >show redundancy detail
Redundancy Management IP Address.................. 9.5.56.10
Peer Redundancy Management IP Address............. 9.5.56.11
Redundancy Port IP Address........................ 169.254.56.10
Peer Redundancy Port IP Address................... 169.254.56.11
Peer Service Port IP Address...................... 0.0.0.0

Redundancy Timeout Values.....:
------------------------------------------------------
Keep Alive Timeout    : 500 msecs
Peer Search Timeout   : 300 secs

Number of Routes.................................. 0

Destination Network          Netmask              Gateway
-------------------    -------------------    -------------------

(Cisco Controller) >
```

352790

キープアライブ タイマー、キープアライブ リトライ、ピア検索タイマーも設定可能で、GUI の [Controller] > [Redundancy] > [Global Configuration] ページから表示できます。

図 24 冗長性のグローバル設定の GUI



352791

Peer RMI ICMP ping を UDP メッセージに変更

リリース 8.0 までは、ピア WLC のハートビートの確認に、冗長性管理インターフェイスの ICMP ping が使用されます。リリース 8.0 では、この機能の一部として、ICMP ping が UDP メッセージに変更されています。

これには、次の要因により利点があります。

- ICMP ping パケットは負荷が重いと廃棄される可能性がある。
- 同じ IP のデバイスが他にあると、ping にも応答する可能性がある。

不正なスイッチオーバーを避けるために、RMI および管理インターフェイスをタグ付けすることをお勧めします。RMI と管理インターフェイスのタギングは、リリース 8.0 では WLC を SSO モードでペアリングする場合に必須になりました。

スタンバイ WLC のオンザフライのメンテナンス モード(MTC)

リリース 8.0 までは、スタンバイ コントローラが「デフォルト ゲートウェイ」または「ピア RP」への到達可能性を失うと、コントローラは再起動して起動中にその状況を確認し、MTC モードを開始します。この機能では、このようなエラー シナリオが発生してもスタンバイ WLC は再起動せず、「オンザフライ(その場)」で MTC モードを開始します。ピア RP とデフォルト ゲートウェイの到達可能性が回復すると、リリース 7.6 で導入された MTC モード自動回復メカニズムが WLC を再起動し、アクティブ WLC とペアリングします。このメカニズムは、スタンバイ WLC でのみ実行されます。アクティブ コントローラの場合は変わらず、MTC モードを開始する前に再起動します。

デフォルト ゲートウェイの到達可能性のチェック機能の強化

この機能強化により、ゲートウェイ(GW)の到達可能性チェック メカニズムは誤検出を回避するように変更されています。また、コントローラの起動時にゲートウェイの到達可能性チェックを実行するタイミングも最適な時期に変更されています。

リリース 8.0 までは、役割のネゴシエーション中に「GW 到達可能性チェック」が実行されていました。リリース 8.0 およびそれ以降では、役割のネゴシエーション中には実行されず、HA ペア設定が完了してから開始されます。

また、特定のスイッチ/ルータ設定のレートで、ICMP ping パケットの制限や破棄が生じることが確認されています。誤検出をトリガーするこのような状況を回避するために、新しい設計では ICMP ping の損失だけでスイッチオーバーの実行を判断しないようになりました。ロジックの変更により、6 回連続して ping が破棄されると、ARP 要求が GW IP アドレスに送信されます。この要求への応答に成功すると、GW は到達可能と見なされます。

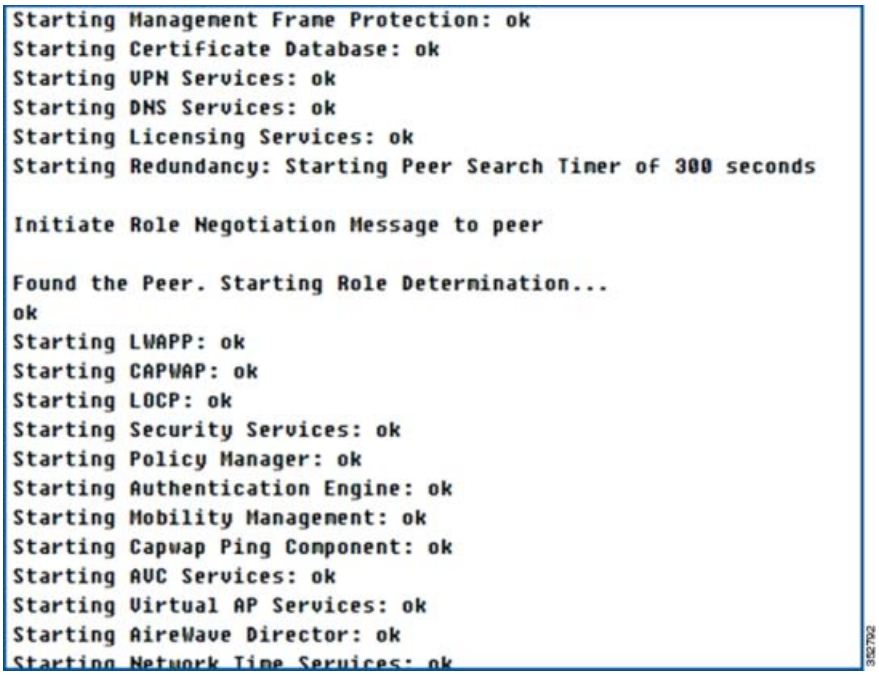
高速 HA ペア設定

現在は、HA のペアリング プロセス時にアクティブ/スタンバイの役割が決まると、アクティブ WLC からスタンバイ WLC に冗長ポートを介して設定が同期されます。設定が異なる場合、セカンダリ WLC は XML の不一致を報告し、アクティブ コントローラから設定をダウンロードしてもう一度リブートします。セカンダリ WLC は、役割が決まった後の次回リブート時に設定を再度検証した上で XML の不一致がないことを報告し、スタンバイ WLC として機能するように処理を続行します。

この機能強化により、XML は初期化時の XML の検証直前に、**アクティブになる**コントローラから**スタンバイになる**コントローラに送信されます。これにより、他のモジュールはまだ初期化されていないため、比較とリブートの余分なステップが避けられ、結果としてアクティブ WLC とスタンバイ WLC のペア設定が高速化されます。

以下のブート ログからわかるように、XML の比較もスタンバイ WLC のリブートも含まれていません。

図 25 スタンバイ WLC のブートアップ ログ



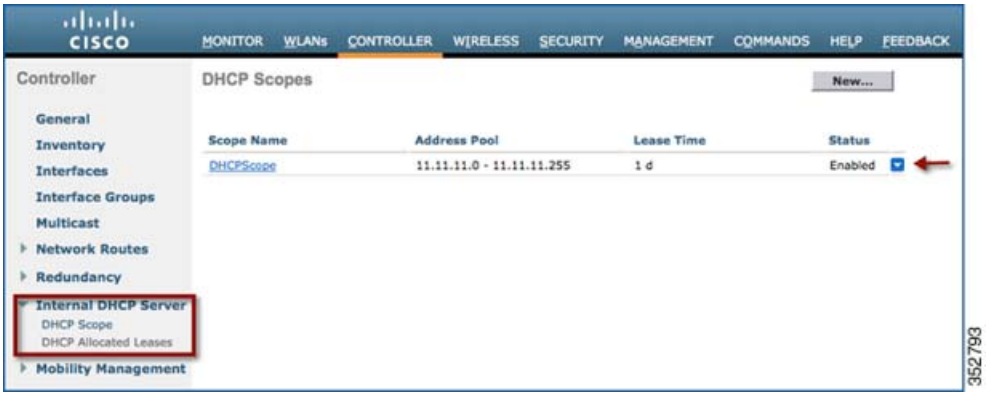
SSO での新しい機能のサポート

内部 DHCP サーバの SSO サポート

リリース 8.0 までは、HA が有効なコントローラに「内部 DHCP サーバ」を構成できません。これは、内部 DHCP サーバのデータがスタンバイ WLC に同期されないためです。リリース 8.0 およびそれ以降では、HA が有効なコントローラに「内部 DHCP サーバ」を構成してデータをスタンバイ WLC に同期できるため、スイッチオーバーの後すぐに、新しいアクティブなコントローラ上の「内部 DHCP サーバ」でクライアントへのサービスを開始できます。

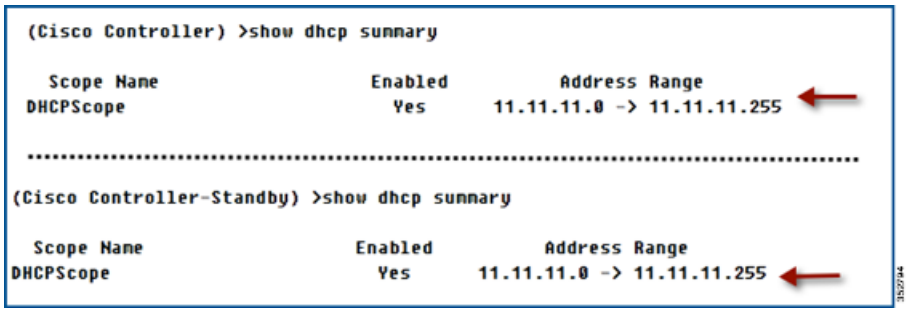
GUI を使用して内部 DHCP サーバを設定するには、[Controller] > [Internal DHCP Server] に移動します。

図 26 内部 DHCP サーバの GUI



同じ内容がスタンバイ コントローラに同期されるので、CLI コマンド **`show dhcp summary`** を実行して確認します。

図 27 アクティブおよびスタンバイ WLC 上の `show dhcp summary`



AP 無線の CAC 統計情報の同期

この機能強化により、音声とビデオ、および通話の統計情報に関する静的な CAC 方式の帯域幅割り当てパラメータがスタンバイ WLC に同期されるため、それぞれの情報はスイッチオーバーの後すぐに、コール アドミッション制御に使用する新しいアクティブ コントローラ上で利用できます。

スリープ状態のクライアントの SSO サポート

リリース 7.5 では、スリープ状態のクライアントの SSO サポートが提供されていませんでした。スリープ状態のクライアント データベースがスタンバイ コントローラに同期されなかったため、スイッチオーバーの発生後はスリープ状態のクライアントを再認証する必要がありました。今回のリリースでは、スリープ状態のクライアント データベースがスタンバイ コントローラに同期されるため、スリープ状態のクライアントは、スリープ状態のクライアント タイムアウト間隔内にスリープ解除された場合、ウェブ再認証を回避できます。

CLI コマンド **`show custom-web sleep-client summary`** を使用して、アクティブ WLC とスタンバイ WLC 間でスリープ状態のクライアント データベースの同期を検証します。

図 28 プライマリ WLC のスリープ状態のクライアント データベース

図 29 スタンバイ WLC のスリープ状態のクライアント データベース

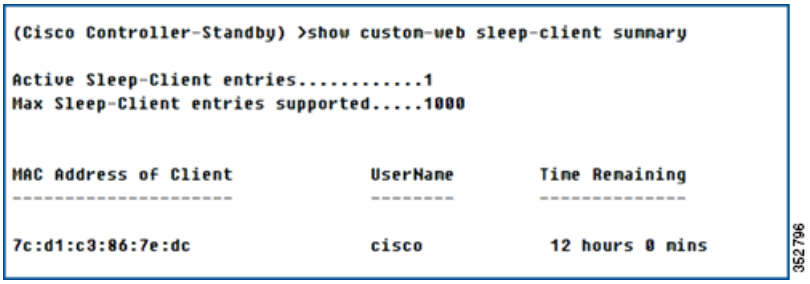


図 30 アクティブおよびスタンバイ WLC のスリープ状態のクライアントの詳細

```
(Cisco Controller) >show custom-web sleep-client detail 7c:d1:c3:86:7e:dc
Mac             : 7c:d1:c3:86:7e:dc
Username        : cisco
Time Left       : 11 hours 40 min
WLAN(SSID)      : enjoy-WebAuth
(Cisco Controller-Standby) >show custom-web sleep-client detail 7c:d1:c3:86:7e:dc
Mac             : 7c:d1:c3:86:7e:dc
Username        : cisco
Time Left       : 11 hours 40 min
WLAN(SSID)      : enjoy-WebAuth
```

352797

OEAP 600 AP の SSO サポート

リリース 8.0 までは、HA ペアでスイッチオーバーが発生すると、OEAP 600 AP は CAPWAP トンネルを再起動して新しいアクティブ コントローラに接続し直すため、接続されているすべてのクライアントの認証は解除されます。この機能により OEAP 600 AP は CAPWAP トンネルをリセットしなくなります。また、クライアントは、新しいアクティブ コントローラとの接続をシームレスに継続します。

以下に示すように、アクティブおよびスタンバイ コントローラで **show ap summary** と **show client summary** コマンドを実行すると、出力に AP とクライアント データベースの同期が表示されます。

図 31 アクティブ WLC 上の OEAP 600 AP

```
(Cisco Controller) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC      Location          Country     IP Address
------------------  -----  -------------------  ----------------  ----------------  ----------  ------------
-
OEAP600              3     AIR-OEAP602I-N-K9    ec:c8:82:b9:6c:60  default location IN       9.5.56.107
```

352798

図 32 スタンバイ WLC への OEAP 600 AP の同期

```
(Cisco Controller-Standby) >show ap summary

Number of APs.................................... 1

Global AP User Name.............................. Not Configured
Global AP Dot1x User Name........................ Not Configured

AP Name             Slots  AP Model             Ethernet MAC      Location          Country     IP Address
------------------  -----  -------------------  ----------------  ----------------  ----------  ------------
OEAP600              3     AIR-OEAP602I-N-K9    ec:c8:82:b9:6c:60  default location IN       9.5.56.107
```

352799

図 33 アクティブ WLC 上のクライアント

```
(Cisco Controller) >show client summary

Number of Clients................................ 1

Number of PMIPV6 Clients......................... 0

                                                  GLAN/
                                                  RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol        Port Wired PMIPV6  Role
----------------- ----------------- ---- ------------ ----- ---- --------------- ---- ----- ------- -------
7c:d1:c3:86:7e:dc OEAP600            1   Associated    1    Yes  802.11n(5 GHz)  1    No    No      Local
```

図 34 スタンバイ WLC へのクライアントの同期

```
(Cisco Controller-Standby) >show client summary

Number of Clients.............................. 1

Number of PMIPV6 Clients....................... 0

                                                GLAN/
                                                RLAN/
MAC Address       AP Name           Slot Status       WLAN  Auth Protocol         Port Wired PMIPV6  Role
----------------- ----------------- ---- ------------ ----- ---- ---------------- ---- ----- ------- ------
7c:d1:c3:86:7e:dc OEAP600            1   Associated    1    Yes  802.11n(5 GHz)   1    No    No      Local
```

リリース 8.1 のハイ アベイラビリティ

リリース 8.1 のハイ アベイラビリティでは、HA スタンバイ モニタリング機能が導入されています。

HA スタンバイ モニタリング機能について

アクティブ コントローラとホット スタンバイ コントローラは、クライアントの観点では 1 つのエンティティと見なされますが、管理者の観点では 2 つの別々 のコントローラと見なして保守、およびモニタします。管理者は、アクティブおよびスタンバイ WLC のステータスと稼働状態を別々に取得し、コントローラのモニタと保守を管理インフラストラクチャとさまざまなユーザ インターフェイスを活用して継続的に行います。

このセクションでは、スタンバイ コントローラから稼働状態に関する情報とトラップを取得するためのインターフェイスについて説明するほか、これらユーザ インターフェイスを CLI、GUI、SNMP から使用する方法について述べます。

イベントと通知

WLC がホット スタンバイになったときのトラップ

トラップは HA ピアがホット スタンバイになったときのタイムスタンプ付きで報告され、次のようなトラップが報告されます。

```
RF notification EventType:37 Reason: HA peer is Hot-Standby...At:Wed Oct 29 18:53:01 2014
```

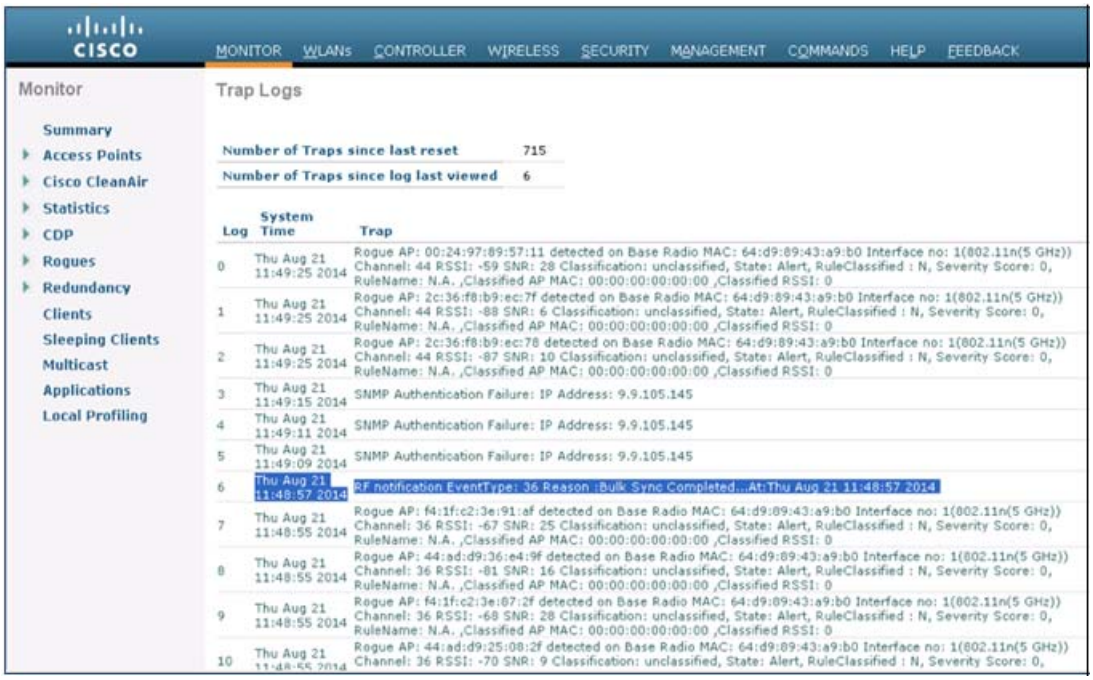
新しいトラップ タイプが CISCO-LWAPP-HA-MIB.my に追加されています。

一括同期が完了したときのトラップ

HA ペアリングが実行され、一括同期が完了すると、次のトラップが報告されます。

```
RF notification EventType:36 Reason: Bulk Sync Completed...At:Wed Oct 29 18:53:16 2014
```

新しいトラップ タイプが CISCO-LWAPP-HA-MIB.my に追加されています。



スタンバイ WLC がダウンしたときのトラップ

スタンバイ ピアが、次のイベントのいずれかによりダウンすると、トラップが報告されます。

- 手動リセット
- クラッシュ時
- メモリ リーク/ハング
- メンテナンス モードへの移行

報告されるトラップは以下のとおりです。

```
RF failure notification ErrorType: 34 Reason :Lost Peer, Moving to Active-No-Peer State!
```

新しいトラップ タイプが CISCO-RF-SUPPLEMENTAL-MIB.my に追加されています。

CLI で、コマンド **show traplog** を実行してトラップを表示できます。

```
(Cisco Controller-Standby) >
Entering Maintenance mode as keepalives are lost..
Keepalive Counters.........:
   ------------------------------------------------------------
   Keepalive requests sent.....................................: 10887
   Keepalive responses received................................: 10884
   Keepalive requests received from peer.......................: 5442
   Keepalive responses sent to peer............................: 5442
   Keepalive requests failed to send...........................: 0
   Keepalive responses failed to send..........................: 0
   Number of times two Keepalives are lost consecutively....: 1
   ------------------------------------------------------------
Entering maintenance mode...

(Cisco Controller) >
*************************************************************
Number of Traps since last reset    63
Number of Traps since log last viewed    63
Log System Time Trap
```

```
0 Mon Oct 6 20:48:08 2014 SNMP Authentication Failure: IP Address: 9.9.105.145
1 Mon Oct 6 20:48:03 2014 RF failure notification ErrorType: 34 Reason :Lost Peer, Moving to Active-No-Peer State!
```

スタンバイでの管理者ログイン時の syslog 通知

SSH を使用したスタンバイへの管理者ログイン

これにより msglog/syslog にイベントが作成されます。メッセージのスニペットは以下のとおりです。

```
*emWeb: Oct 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="SSH"] user login success on standby controller.
```

このメッセージは、CLI の「**show msglog**」を実行して、スタンバイ WLC で表示できます。

```
(Cisco Controller-Standby) >show msglog
Message Log Severity Level .....................VERBOSE
*emWeb: Oct 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="SSH"] user login success on standby controller.
```

コンソールを使用したスタンバイへの管理者ログイン

これにより msglog/syslog にイベントが作成されます。メッセージのスニペットは以下のとおりです。

```
*emWeb: Oct 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="console"] user login success on standby controller.
```

このメッセージは、CLI の「**show msglog**」を実行して、スタンバイ WLC で表示できます。

```
(Cisco Controller-Standby)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration to factory defaults)

User:  admin
Password:*****
User login success on standby
Your password does not meet the strong password requirements.For added security, set a new password that meets these requirements.To prevent this message from showing again, disable the strong password feature.
(Cisco Controller-Standby) >
(Cisco Controller-Standby) >show msglog
Message Log Severity Level .....................VERBOSE
*emWeb: Oct 06 20:34:42.675: #CLI-3-LOGIN_STANDBY: [SS] cli_lvl7.c:4520 [USER@9 name="admin" from="console"] user login success on standby controller.
```

CLI のピア プロセス統計情報

この機能により、スタンバイ WLC のすべてのスレッドの CPU とメモリの統計情報がアクティブ コントローラに 10 秒ごとに同期されます。この情報は、ユーザがアクティブ WLC 上のピア統計情報を照会したときに表示されます。

アクティブ WLC でピア プロセスのシステム、CPU、メモリの統計情報を表示するための新しいコマンドは次のとおりです。

- **show redundancy peer-system statistics**
- **show redundancy peer-process cpu**
- **show redundancy peer-process memory**

```
(Cisco Controller) >show redundancy peer-system statistics
Peer System CPU statistics:Current CPU(s) load: 0%
Individual CPU load: 0%/1%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%

Peer System Memory Statistics:
Total System Memory.............: 1025646592 bytes (978.20 MB)
Used System Memory..............: 544792576 bytes (519.59 MB)
Free System Memory..............: 480854016 bytes (458.61 MB)
Bytes allocated from RTOS......: 89576252 bytes (85.43 MB)
Chunks Free.....................: 316 bytes
Number of mmapped regions......: 48
Total space in mmapped regions.: 293515264 bytes (279.93 MB)
Total allocated space..........: 28793316 bytes (27.46 MB)
Total non-inuse space..........: 60782936 bytes (57.97 MB)
Top-most releasable space......: 810440 bytes (791.44 KB)
Total allocated (incl mmap)....: 383091516 bytes (365.37 MB)
Total used (incl mmap).........: 322308580 bytes (307.39 MB)
Total free (incl mmap).........: 60782936 bytes (57.97 MB)
Peer system Power supply statistics:
Power Supply 1.................................Present, OK
Power Supply 2.................................Absent
```

これらの統計情報を取得するために MIB CISCO-LWAPP-HA-MIB.my が更新されています。

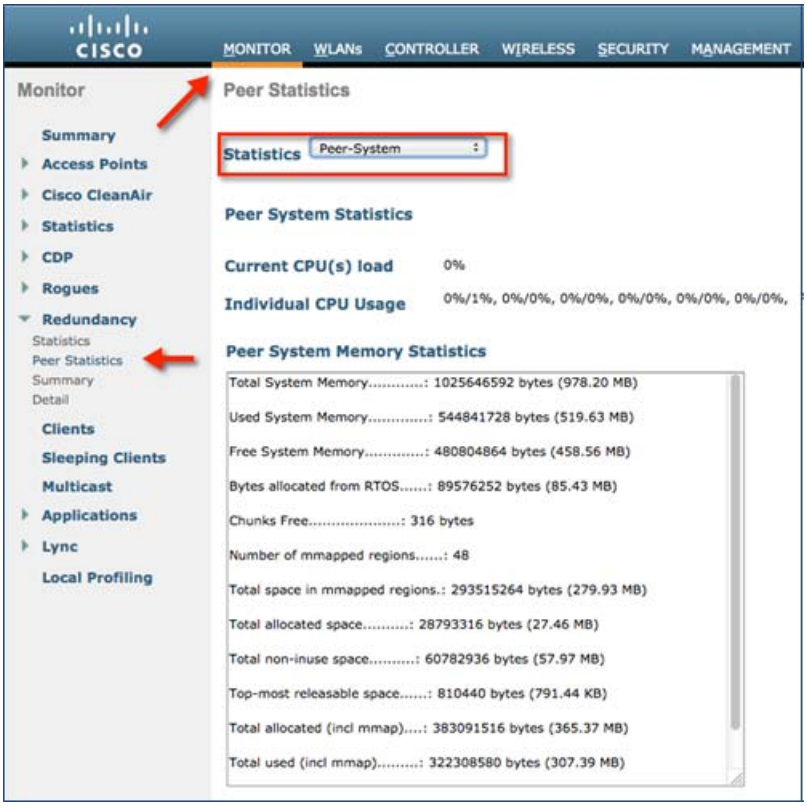
```
(Cisco Controller) >show redundancy peer-process cpu

   Name                 PID   Priority      CPU Use    (usr/sys)% hwm   CPU   Reaper

   System Reset Task    3161    (240/  7)        0      (  0/  0)%    0     2
   reaperWatcher        3160    (  3/ 96)        0      (  0/  0)%    0     2    I
   osapiReaper          3159    ( 10/ 94)        0      (  0/  0)%    0     2    I
   TempStatus           3158    (240/  7)        0      (  0/  0)%    0     7    I
   rsyncmgrSndqTask     3142    ( 90/ 64)        0      (  0/  0)%    0     6
   rsyncmgrHoldqTask    3141    ( 90/ 64)        0      (  0/  0)%    0     2
   rsyncmgrRcvqTask     3139    ( 90/ 64)        0      (  0/  0)%    0     4
   pktDebugSocketTask   3133    (255/  1)        0      (  0/  0)%    0     4
   webauthRedirect      3132    (240/  7)        0      (  0/  0)%    0     3
   emWeb                3131    (240/  7)        0      (  0/  0)%    0     3
   mdnsHATask           3129    (240/  7)        0      (  0/  0)%    0     4
   Bonjour_Socket_Tas   3128    (240/  7)        0      (  0/  0)%    0     4
   Bonjour_Process_Ta   3127    (174/ 32)        0      (  0/  0)%    0     4
   Bonjour_Msg_Task     3126    (174/ 32)        0      (  0/  0)%    0     4
   portalMonitorMsgTa   3125    (240/  7)        0      (  0/  0)%    0     6
   portalMsgTask        3124    (240/  7)        0      (  0/  0)%    0     2
   portalSockTask       3123    (240/  7)        0      (  0/  0)%    0     2
   iWAG GTP Audit Man   3121    (240/  7)        0      (  0/  0)%    0     3
   iWAG GTP PDP direc   3120    (240/  7)        0      (  0/  0)%    0     2
   PMIPV6_Thread_3      3119    (240/  7)        0      (  0/  0)%    0     2
   PMIPV6_Thread_2      3118    (240/  7)        0      (  0/  0)%    0     2
   PMIPV6_Thread_1      3117    (240/  7)        0      (  0/  0)%    0     2
   PMIPV6_Thread_0      3116    (240/  7)        0      (  0/  0)%    0     2
   hotspotTask          3115    (100/ 60)        0      (  0/  0)%    0     2
   ipv6SocketTask       3109    (240/  7)        0      (  0/  0)%    0     5
   HAConfigSyncTask     3110    (240/  7)        0      (  0/  0)%    0     6
   IPv6_Msg_Task        3108    (174/ 32)        0      (  0/  0)%    0     1
   sisfSwitcherTask     3107    (174/ 32)        0      (  0/  0)%    0     1

(Cisco Controller) >show redundancy peer-process memory
```

```
Name                 Priority       BytesInUse  BlocksInUse     Reaper

System Reset Task   (240/  7)              0            0       (  0/  0)%
reaperWatcher       (  3/ 96)              0            0       (  0/  0)%    I
osapiReaper         ( 10/ 94)              0            0       (  0/  0)%    I
TempStatus          (240/  7)            428            1       (  0/  0)%    I
rsyncmgrSndqTask    ( 90/ 64)          24930            5       (  0/  0)%
rsyncmgrHoldqTask   ( 90/ 64)              0            0       (  0/  0)%
rsyncmgrRcvqTask    ( 90/ 64)              0            0       (  0/  0)%
pktDebugSocketTask  (255/  1)              0            0       (  0/  0)%
webauthRedirect     (240/  7)        1240549          603       (  0/  0)%
emWeb               (240/  7)         501136         8844       (  0/  0)%
mdnsHATask          (240/  7)              0            0       (  0/  0)%
Bonjour_Socket_Tas  (240/  7)              0            0       (  0/  0)%
Bonjour_Process_Ta  (174/ 32)              0            0       (  0/  0)%
Bonjour_Msg_Task    (174/ 32)              0            0       (  0/  0)%
portalMonitorMsgTa  (240/  7)              0            0       (  0/  0)%
portalMsgTask       (240/  7)              0            0       (  0/  0)%
portalSockTask      (240/  7)              0            0       (  0/  0)%
iWAG GTP Audit Man  (240/  7)           2078            6       (  0/  0)%
iWAG GTP PDP direc  (240/  7)          10414           13       (  0/  0)%
PMIPV6_Thread_3     (240/  7)           2986           18       (  0/  0)%
PMIPV6_Thread_2     (240/  7)           2986           18       (  0/  0)%
PMIPV6_Thread_1     (240/  7)           2986           18       (  0/  0)%
PMIPV6_Thread_0     (240/  7)           5738           36       (  0/  0)%
hotspotTask         (100/ 60)              0            0       (  0/  0)%
ipv6SocketTask      (240/  7)              0            0       (  0/  0)%
HAConfigSyncTask    (240/  7)            312            4       (  0/  0)%
IPv6_Msg_Task       (174/ 32)              0            0       (  0/  0)%
sisfSwitcherTask    (174/ 32)             36            1       (  0/  0)%
SISF Feature Proce  (240/  7)              0            0       (  0/  0)%
SISF BT Process     (174/ 32)             16            1       (  0/  0)%
fmcHsTask           (100/ 60)              0            0       (  0/  0)%
```

GUI のピア プロセス統計情報

GUI のピア統計情報は、[Monitor] > [Redundancy] > [Peer Statistics] で表示できます。

図 35 ピア プロセスのシステム統計情報



これらの統計情報を取得するために MIB CISCO-LWAPP-HA-MIB.my が更新されています。

図 36 ピア プロセスの CPU 統計情報

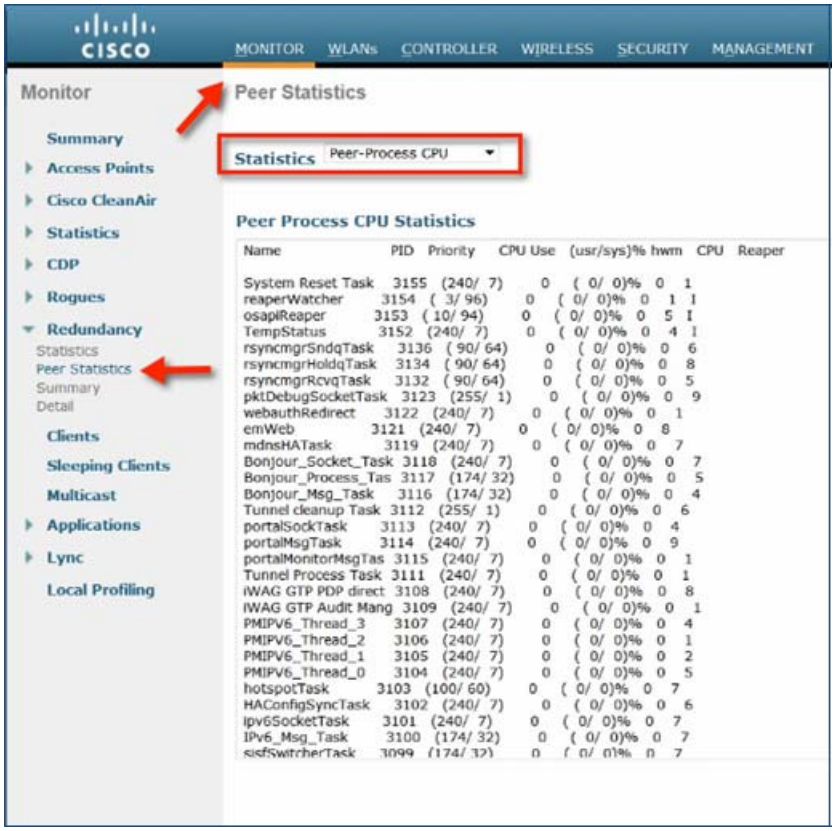
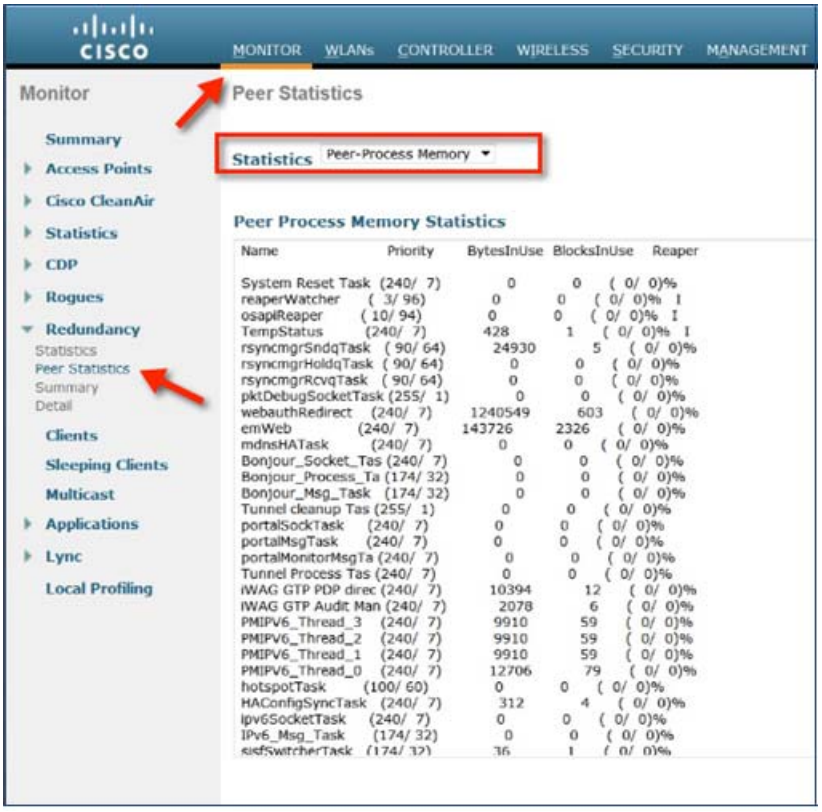


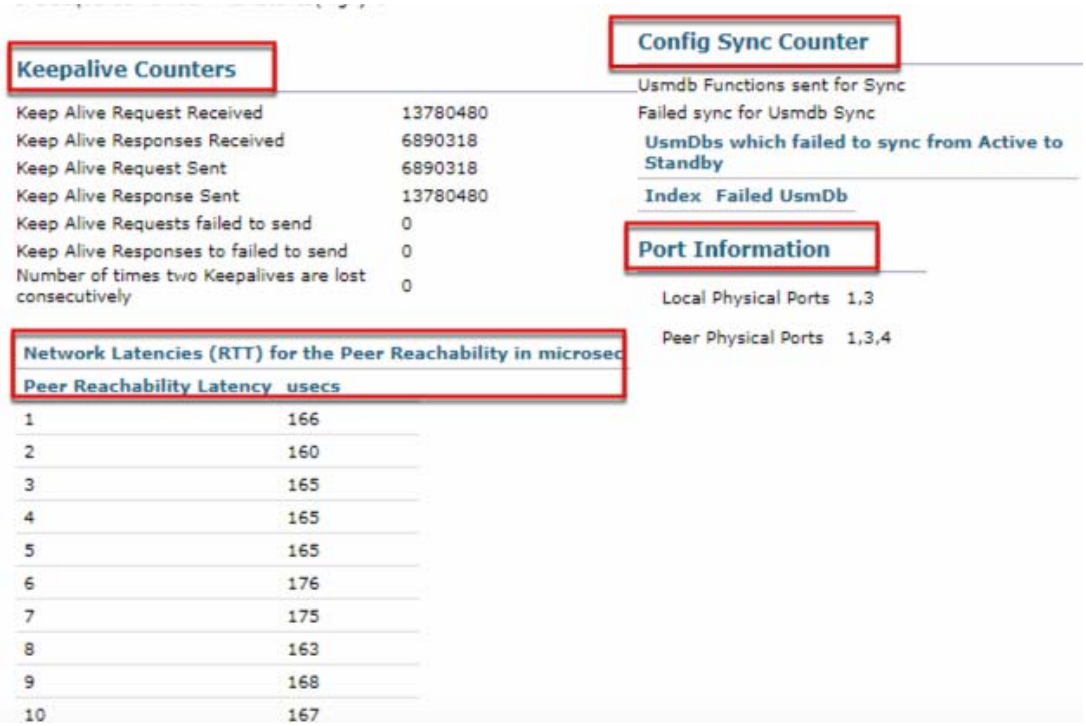
図 37 ピア プロセスのメモリ統計情報

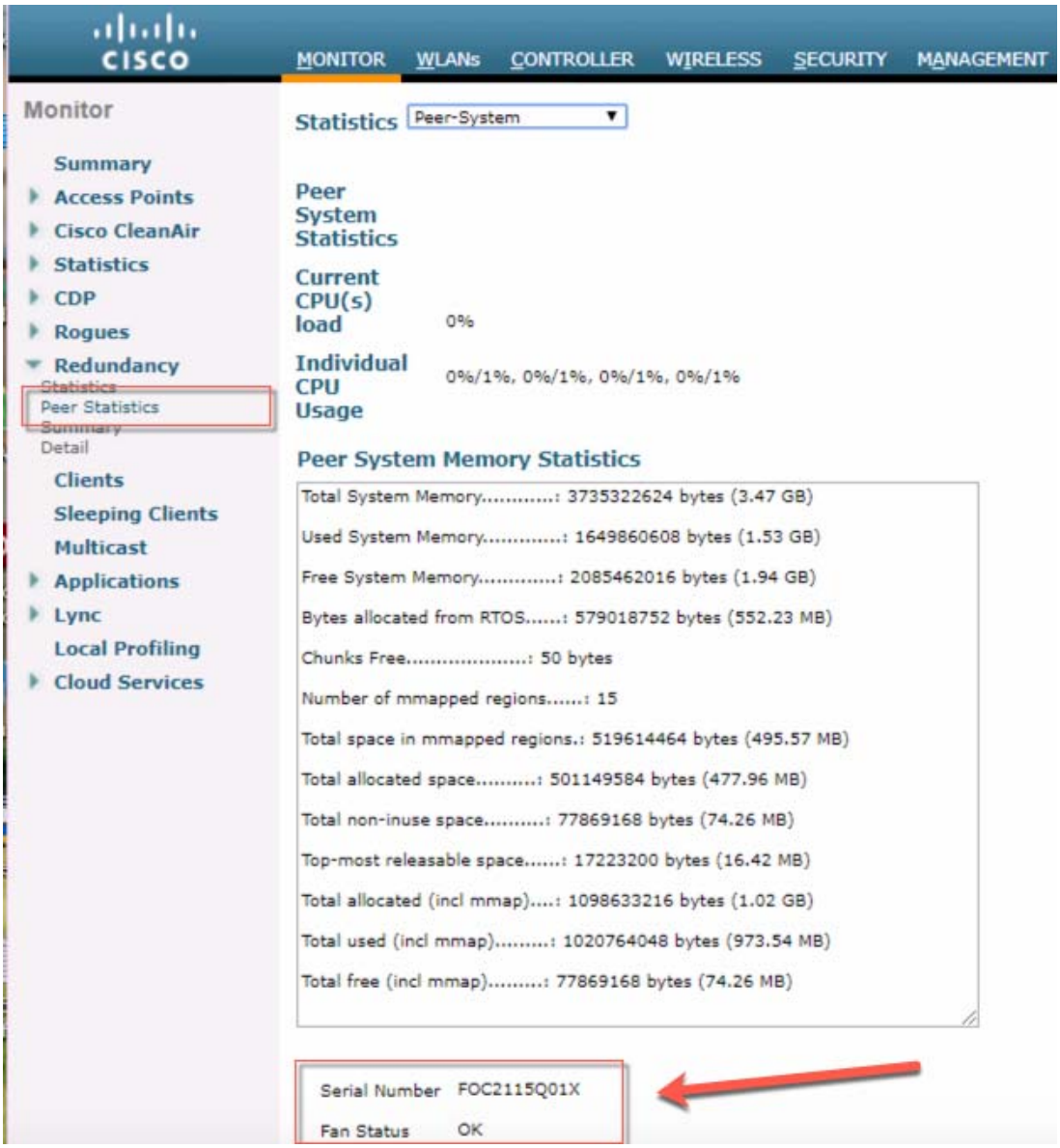
リリース 8.7 の HA モニタリングの機能強化

SNMP MIB を含む Management では、以下で説明する統計情報を取得するように MIB CISCO-LWAPP-HA-MIB.my が更新されています。

コントローラの [Monitor] タブに移動し、[Redundancy] を選択して統計情報をモニタできます。


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Redundancy
Statistics
Peer Statistics
Summary
Detail
Clients
Sleeping Clients
Multicast
Applications
Lync
Local Profiling
Peer Statistics
Statistics Peer-Process Memory
Peer Process Memory Statistics
Name Priority BytesInUse BlocksInUse Reaper
System Reset Task (240/ 7) 0 0 (0/ 0)%
reaperWatcher (3/ 96) 0 0 (0/ 0)% I
osapiReaper (10/ 94) 0 0 (0/ 0)% I
TempStatus (240/ 7) 428 1 (0/ 0)% I
rsyncmgrSndqTask (90/ 64) 24930 5 (0/ 0)%
rsyncmgrHoldqTask (90/ 64) 0 0 (0/ 0)%
rsyncmgrRcvqTask (90/ 64) 0 0 (0/ 0)%
pktDebugSocketTask (255/ 1) 0 0 (0/ 0)%
webauthRedirect (240/ 7) 1240549 603 (0/ 0)%
emWeb (240/ 7) 143726 2326 (0/ 0)%
mdnsHATask (240/ 7) 0 0 (0/ 0)%
Bonjour_Socket_Tas (240/ 7) 0 0 (0/ 0)%
Bonjour_Process_Ta (174/ 32) 0 0 (0/ 0)%
Bonjour_Msg_Task (174/ 32) 0 0 (0/ 0)%
Tunnel cleanup Tas (255/ 1) 0 0 (0/ 0)%
portalSockTask (240/ 7) 0 0 (0/ 0)%
portalMsgTask (240/ 7) 0 0 (0/ 0)%
portalMonitorMsgTa (240/ 7) 0 0 (0/ 0)%
Tunnel Process Tas (240/ 7) 0 0 (0/ 0)%
iWAG GTP PDP direc (240/ 7) 10394 12 (0/ 0)%
iWAG GTP Audit Man (240/ 7) 2078 6 (0/ 0)%
PMIPV6_Thread_3 (240/ 7) 9910 59 (0/ 0)%
PMIPV6_Thread_2 (240/ 7) 9910 59 (0/ 0)%
PMIPV6_Thread_1 (240/ 7) 9910 59 (0/ 0)%
PMIPV6_Thread_0 (240/ 7) 12706 79 (0/ 0)%
hotspotTask (100/ 60) 0 0 (0/ 0)%
HAConfigSyncTask (240/ 7) 312 4 (0/ 0)%
ipv6SocketTask (240/ 7) 0 0 (0/ 0)%
IPv6_Msg_Task (174/ 32) 0 0 (0/ 0)%


Keepalive Counters
Keep Alive Request Received 13780480
Keep Alive Responses Received 6890318
Keep Alive Request Sent 6890318
Keep Alive Response Sent 13780480
Keep Alive Requests failed to send 0
Keep Alive Responses to failed to send 0
Number of times two Keepalives are lost consecutively 0
Config Sync Counter
Usmdb Functions sent for Sync
Failed sync for Usmdb Sync
UsmDbs which failed to sync from Active to Standby
Index Failed UsmDb
Port Information
Local Physical Ports 1,3
Peer Physical Ports 1,3,4
Network Latencies (RTT) for the Peer Reachability in microsec
Peer Reachability Latency usecs
1 166
2 160
3 165
4 165
5 165
6 176
7 175
8 163
9 168
10 167



Web リンク

- Cisco WLAN コントローラ情報:
  http://www.cisco.com/c/en/us/products/wireless/4400-series-wireless-lan-controllers/index.html
  http://www.cisco.com/c/en/us/products/wireless/2000-series-wireless-lan-controllers/index.html
- Cisco NCS 管理ソフトウェア情報:
  http://www.cisco.com/c/en/us/products/wireless/prime-network-control-system-series-appliances/index.html
- Cisco MSE 情報:http://www.cisco.com/c/en/us/products/wireless/mobility-services-engine/index.html
- Cisco LAP ドキュメンテーション:http://www.cisco.com/c/en/us/products/wireless/aironet-3500-series/index.html

用語

- APM:AP マネージャ インターフェイス
- Dyn:ダイナミック インターフェイス
- Management:管理インターフェイス
- ポート:物理 Gbps ポート
- WiSM-2:ワイヤレス サービス モジュール
- AP:アクセス ポイント
- LAG:Link Aggregation(リンク集約)
- SPAN:Switch Port Analyzer(スイッチド ポート アナライザ)
- RSPAN:リモート SPAN
- VACL:VLAN アクセス コントロール リスト
- DEC:Distributed Etherchannel(分散型 Etherchannel)
- DFC:Distributed Forwarding Card(分散型フォワーディング カード)
- OIR:Online Insertion and Removal(オンライン活性挿抜)
- VSL:Virtual Switch Link(仮想スイッチ リンク)
- ISSU:In Service Software Upgrade(インサービス ソフトウェア アップグレード)
- MEC:Multichassis Ether Channel(マルチシャーシ EtherChannel)
- VSS:Virtual Switch System(仮想スイッチ システム)
- WCS:Wireless Control System(ワイヤレス制御システム)
- NAM:Network Analysis Module(ネットワーク解析モジュール)
- IDSM:Intrusion Detection Service Module(侵入検知サービス モジュール)
- FWSM:Firewall Service Module(ファイアウォール サービス モジュール)
- STP:Spanning Tree Protocol(スパニング ツリー プロトコル)
- VLAN:仮想 LAN
- SSO:Stateful Switchover(ステートフル スイッチオーバー)
- WCP:Wireless Control Protocol(ワイヤレス制御プロトコル)
- WiSM-2:ワイヤレス サービス モジュール-2

用語集

A

AP SSO
アクセス ポイント ステートフル スイッチオーバーでは、各 AP の CAPWAP 状態がアクティブ WLC とスタンバイ WLC で維持され、スタンバイ WLC へのスイッチオーバー後にも CAPWAP 状態が維持されます。フェールオーバー後に AP の CAPWAP 探索と接続のプロセスは不要です。

P

Peer
AP SSO はボックスツーボックス冗長性(1 対 1)であるため、HA セットアップの両方の WLC(アクティブとスタンバイ)は、相互にピアになります。

あ

アクティブ WLC
HA ペアで現在アクティブであり、ワイヤレス ネットワークを処理している WLC。AP は、アクティブ WLC との単一 CAPWAP トンネルを確立します。

き

キープアライブ タイマー
HA セットアップ中のスタンバイ WLC は、アクティブ WLC の状態を検査するキープアライブ パケットを冗長ポートで送信します。アクティブ WLC からの 3 個のキープアライブ パケットの確認応答がなかった場合、スタンバイはアクティブをダウンと宣言し、ネットワークを引き継ぎます。

く

クライアント SSO
ワイヤレス クライアント ステートフル スイッチオーバーでは、クライアント状態もアクティブおよびスタンバイ WLC で維持され、スイッチオーバー後にもワイヤレス クライアントは認証解除されません。将来のリリースでサポートされる予定です。

じ

冗長 VLAN
アクティブとスタンバイの WLC 間での HA 役割のネゴシエーションなど、設定と冗長性メッセージの交換のために Catalyst 6000 バックプレーンに接続された WiSM-2 冗長ポート用に Catalyst 6500 スーパーバイザに作成された VLAN。

冗長性管理インターフェイス
HA セットアップの両方の WLC 上の管理インターフェイスへのパラレルインターフェイス。管理インターフェイスと同じサブネットにある必要があります。このインターフェイスによって、スタンバイ WLC ではインフラ ネットワークと対話でき、アクティブとスタンバイの WLC 間でインフラ ネットワーク越しにいくつかの冗長性メッセージを交換することもできます。

冗長ポート
HA 役割のネゴシエーション、設定の同期、およびアクティブとスタンバイの WLC 間の冗長性メッセージで使用する、5500/7500/8500 WLC 上の物理ポート。

す

スタンバイ WLC
HA ペアのアクティブ コントローラをモニタしており、アクティブ WLC の故障時にワイヤレス ネットワークを引き継ぐ準備ができている WLC。

せ

セカンダリ ユニット AP SSO 導入では、実行している永久カウント ライセンスの数が少ないか等しいコントローラはセカンダリ ユニットとして設定される必要があり、HA SKU UDI(AP カウント ライセンスがゼロ)を持つコントローラは、デフォルトでセカンダリ ユニットとして出荷されています。セカンダリ ユニットは WLC であり、HA ペアを初めて形成したときにスタンバイ WLC の役割を引き受けます。セカンダリ ユニットは、冗長ポートを介して、ピア(アクティブ WLC)からライセンス カウント情報を継承します。

ぴ

ピア検索タイマー スタンバイ WLC では、ブート時にピアを検出するためにピア検索タイマーの長さ(デフォルトは 2 分)待機します。この時間内にピアを検出できない場合、WLC では、状態をメンテナンス モードに遷移します。

ぷ

プライマリ ユニット AP SSO 導入では、実行している永久カウント ライセンスの多い側のコントローラをプライマリ ユニットとして設定する必要があります。プライマリ ユニットは WLC であり、HA ペアを初めて形成したときにアクティブ WLC の役割を引き受けます。プライマリ ユニットは、冗長ポートを介してピアにライセンス カウント情報を送信します。

め

メンテナンス モード スタンバイ WLC がゲートウェイと通信できない、または冗長ポートを介してピア WLC(アクティブ WLC)を検出できない場合、メンテナンス モードに入ります。このモードでは、WLC はインフラ ネットワークと通信できず、HA 処理に参加しません。メンテナンス モードの WLC は HA 処理に参加しないため、メンテナンス モードを終了して HA 処理に再度参加するには、手動でリブートする必要があります。

も

モビリティ MAC HA セットアップのピア間で共有される一意な MAC アドレス。この MAC アドレスは、HA セットアップと、HA セットアップの別の WLC の間または独立したコントローラの間のモビリティ ペアを形成するために使用する必要があります。デフォルトでは、アクティブ WLC の MAC アドレスがモビリティ MAC アドレスとして共有されますが、CLI を使用してアクティブ WLC にモビリティ MAC を手動で設定することでもできます。このモビリティ MAC は HA セットアップのピア間で共有されます。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems
- N+1 導入ガイド