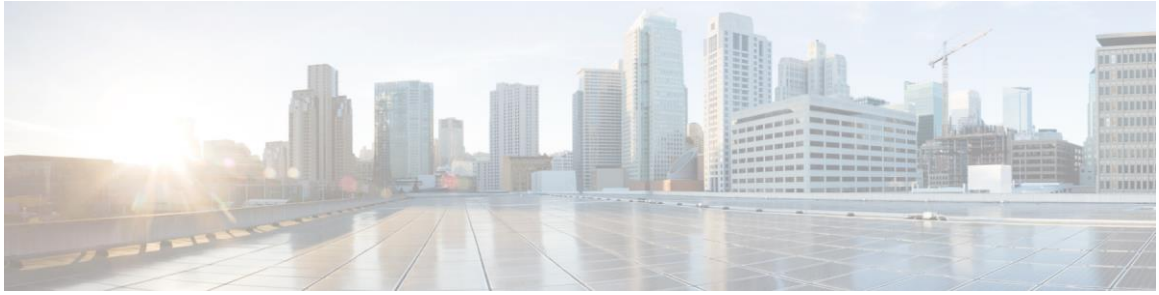


无线控制器高可用性（SSO）部署指南（7.5版本）

Last Updated: August, 2013
Release: High Availability (SSO) Deployment Guide Release 7.5

原文链接：http://www.cisco.com/en/US/partner/docs/wireless/controller/technotes/7.5/High_Availability_DG.html
翻译人：冯博
校对：谢清
译于2013年10月

简介

本文档提供了有关思科统一无线控制器（WLC）操作和配置的理论，它涉及到了支持无线接入点和客户端状态化故障切换（SSO）。

新的高可用性（HA）功能（即AP SSO）可以在思科统一无线网络软件7.3和7.4版本中进行设置，允许无线接入点与活动的无线控制器建立CAPWAP隧道，并与备用无线控制器共享无线接入点的数据库镜像副本。当主用无线控制器失效，并且待机无线控制器接管网络成为主用无线控制器之后，无线接入点不会进入到发现状态。无线接入点和在Active状态的无线控制器之间在同一时间只能维持一个CAPWAP隧道。新增的无线接入点SSO功能的目的是为了在思科统一无线网络由于机箱或者网络故障的时候，减少主控制器的停机时间。

为了支持不影响服务的高可用性，就需要支持无线接入点和客户端从主控制器无缝的切换到备用控制器。7.5版本支持无线控制器的客户端无状态切换（客户端SSO）。客户端的SSO功能是在客户端已经完成了认证授权和DHCP阶段，并且已经开始发送数据后生效。客户端的SSO功能，在当客户端与无线控制器关联或者是客户端参数变化的时候，备用控制器的客户端的信息就会被同步。完全认证的客户端，比如，在运行状态的客户端就会与备用控制器同步，所以无线接入点和客户端在无缝切换控制器的时候就不需要再进行认证了，这样就实现了无服务中断以及无SSID中断。

先决条件

需求

本文档没有特殊的需求。

使用的组件

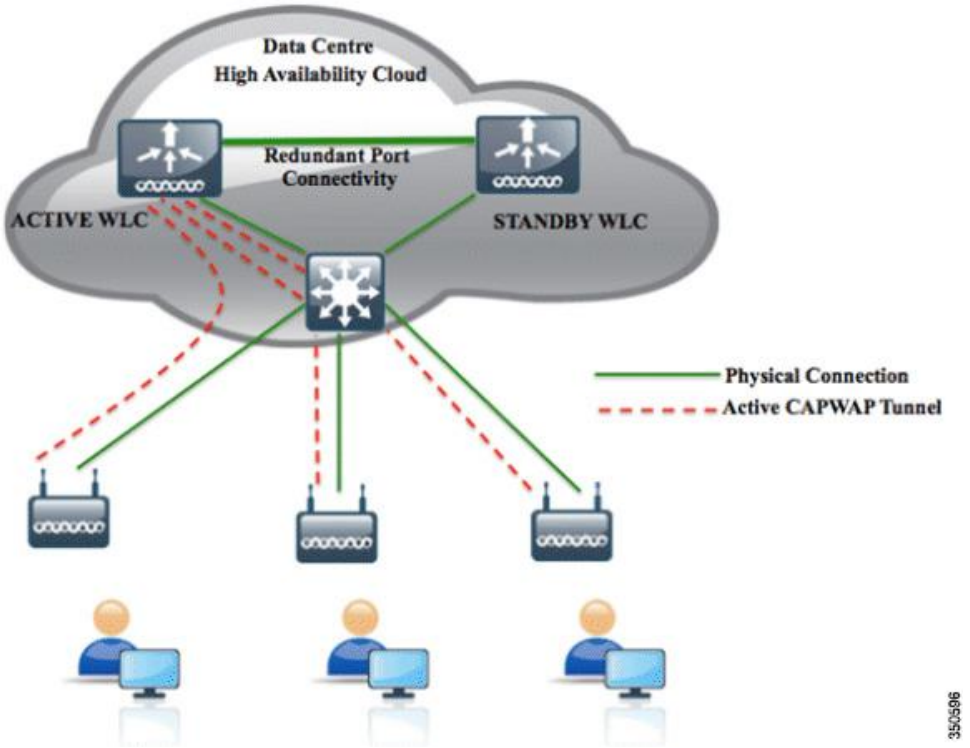
本文档中的信息是基于以下软件和硬件版本：

- 无线控制器5500系列，7500/8500系列，以及WiSM-2系列无线控制器模块
- 700，1130,1240,1250,1040,1140,1260,1600,2600,3500,3600系列无线接入点，以及1520和1550系列Mesh无线接入点（MAP）

本文档中的信息是在一个特定的实验室环境中的设备上生成的。本文档中使用的所有设备以缺省（默认）配置开始配置。如果您的网络是正在使用的生产系统，请确保您了解所有的命令会带来的潜在影响。

拓扑

本文档使用如下网络拓扑



新的高可用性特性概述

新高可用性架构用于机箱冗余。换句话说就是主备1:1的配置，一个无线控制器处于活动状态，另一个无线控制器为热备状态，通过无线控制器上的冗余端口持续监测主用无线控制器的运行状态。两台无线控制器共享同一组一样的配置，包括了管理接口的IP地址。待机无线控制器不需要独立配置，只需要通过主用无线控制器的冗余端口就可以同步所有配置状态（在启动的时候使用Bulk批量配置，在运行的时候使用增量配置）。无线接入点的CAPWAP状态（只有处在运行状态的无线接入点）也会进行同步，无线接入点数据库的镜像副本会保存在备无线控制器上。当主用无线控制器故障，待机无线控制器接管网络成为主用无线控制器时，无线接入点不会进入发现状态。

在这里没有抢占功能。当以前的主用无线控制器恢复工作的时候，它不会变回成主用无线控制器，只会与现有主用无线控制器协商自己的状态并成为备用状态的控制器。活动和备用状态的决定不是一个自动选举过程。从7.3版本开始，是根据HA设备的SKU（生产序号UDI）来决定活动/备用无线控制器。一个有HA SKU UDI的无线控制器第一次启动并和一个运行永久计数许可的无线控制器搭配使用时，它将始终是备用无线控制器。对于现有的配备了永久计数许可的无线控制器，可以通过手动配置决定活动/备用的状态。

在5500/7500/8500系列的无线控制器和WiSM-2上都支持AP SSO功能。7.3版本仅支持AP SSO，可以保证切换后无线接入点进程的完整。Mesh无线接入点（MAP），被视为RAP上的Mesh客户端，在AP SSO时不会进行重新认证。

客户端SSO功能在7.5版本及以后支持，在5500/7500/8500系列的无线控制器和WiSM-2上都是支持的，请参考7.5版本的高可用性文档

使用冗余端口连接实现5500/7500/8500系列无线控制器的高可用性

- 在5500/7500/8500系列无线控制器上有一个专用的冗余端口用作背靠背连接，用来同步从主用无线控制器到备用无线控制器上的配置。

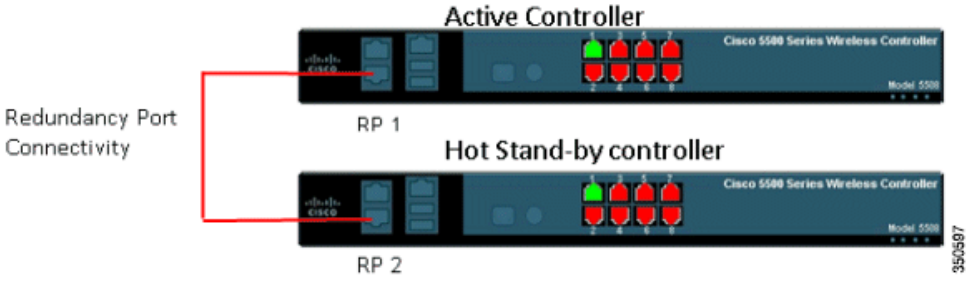
- 备用无线控制器每100毫秒（默认定时器）都会通过冗余端口向主用无线控制器发送心跳报文

以检查主用无线控制器的运行健康状态。

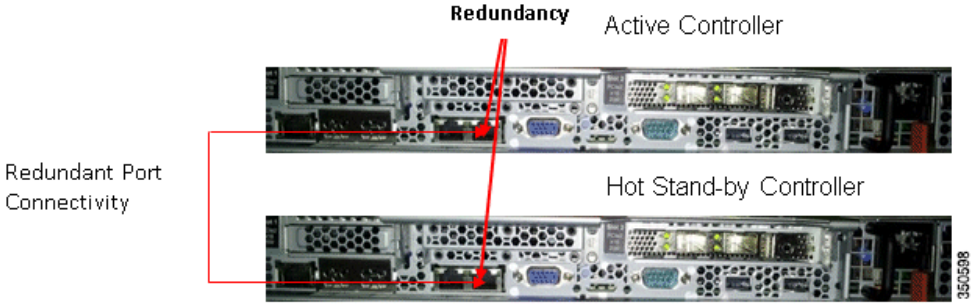
- 在HA设置里的两个无线控制器都会跟踪网关的可达性。主用无线控制器会用管理IP地址作为源地址发送因特网控制消息协议（ICMP）包来ping网关，备用无线控制器使用冗余管理IP地址向网关发送一个ICMP来ping网关。两个无线控制器每隔一秒钟的时间间隔发送一个ICMP包来ping网关。

- 强烈建议使用冗余端口之间用背靠背直接连接。

可以从下图中看到5500系列无线控制器在HA配置下的冗余端口连接情况：



可以从下图中看到7500系列无线控制器在HA配置下的冗余端口连接情况：



注意

强烈建议主备冗余端口之间采用直接物理链路连接。在每个以太网电缆标准端口之间的连接距离可以达100米

使用冗余VLAN连接实现WiSM-2无线控制模块的高可用性

- WiSM-2无线控制器上有一个专门的冗余VLAN用于主用无线控制器到备用无线控制器的配置的同步。

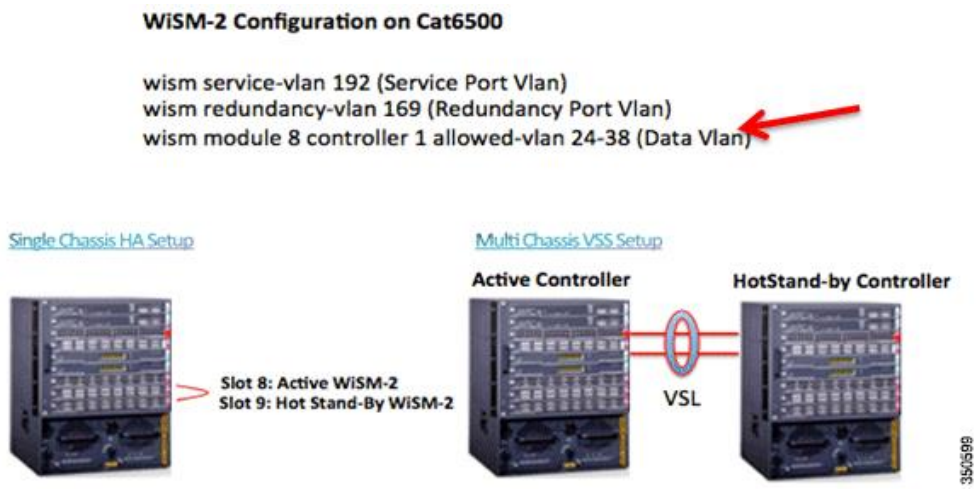
- 冗余VLAN是用作高可用性配对过程的二层专属VLAN。它不应该跨越网段，也不应该有任何3层SVI接口。不能用数据VLAN当做冗余VLAN。

- 备用无线控制器每100毫秒（默认定时器）通过冗余VLAN向主用无线控制器发送心跳报文，以检查主用无线控制器的运行健康状况。

- 配置为HA的WiSM模块会跟踪网关的可达性。主用无线控制器使用管理IP地址作为源地址向网关发送一个ICMP包来ping网关，备用无线控制器使用的冗余管理IP地址向网关发送一个ICMP包来ping网关。两个无线控制器每隔一秒钟的时间间隔发送一个ICMP包来ping网关。

- 为了实现高可用性，两块WiSM-2无线控制器应该部署在一个单机箱中或部署在使用了VSS连接的两台Catalyst 6500机箱上。

下图显示了在一个机箱中的高可用性连接和扩展到VSS多机箱上的冗余VLAN：



注意

冗余VLAN必须是一个路由不可达的VLAN。换句话说，这个VLAN上没有3层接口，并且可以在VSS组内的多机箱上通过建立VSL链路来扩展HA设置。重要的是要确保该VLAN是专用的HA VLAN，不属于任何数据VLAN，否则可能会导致不可预测的结果。

注

建立冗余VLAN应该像在IOS®交换机上建立任何正常的数据VLAN一样。冗余VLAN是为WiSM-2卡连接到背板的冗余端口配置的。没有必要为冗余VLAN配置IP地址，因为它会收到一个自动生成的IP地。这在本文档后面部分会有讨论。

注

在思科WiSM2和Catalyst 6500系列Supervisor引擎2T上，如果启用了高可用性，发生了控制器角色切换，无线接入点有可能断开，然后再与WiSM2无线控制器关联。为了防止这种情况的发生，在你配置高可用性前，我们建议您在Port Channel中，检查主活动的和备用思科WiSM2无线控制器的细节，确保端口是以相同的顺序均衡的，并且Port Channel的Hash分布使用的是固定算法。如果它们排列顺序不对，你必须将Port Channel的分布改成固定算法，然后从Cisco Catalyst 6500系列2T引擎上重启WiSM2无线控制器。您可以使用命令show etherchannel prot-channel来验证端口顺序和负载值。您可以使用配置命令port-channel hash-distribution fixed使分布固定。

注

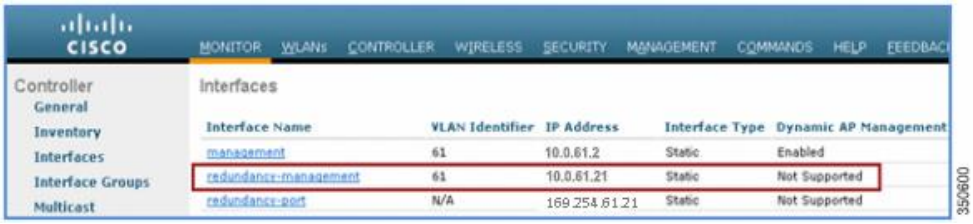
在7.5版本中，要支持不同数据中心中主控制器和备用控制器的高可用性，冗余端口的背对背连接不再是必须的了，可用将冗余端口连接到交换机，使得无线控制器是2层邻接。详请参见7.5版本的冗余端口连接一章。

高可用性互动新接口的介绍

冗余管理接口

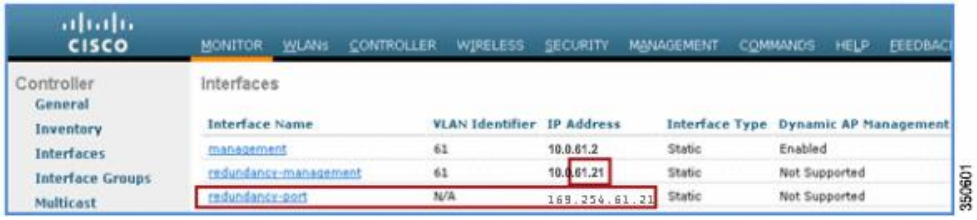
该接口上的IP地址应该与管理接口在同一个子网里。该接口会通过网络基础设施通过主用

无线控制器是否回应冗余端口上的保持活动状态信息来监控主用无线控制器的状态。这提供了额外的健康检查来确认主用无线控制器的运行状态，并确认切换是否该被执行。此外，备用无线控制器使用这个接口作为源地址来发送ICMP ping包检查网关的可达性。如果机箱故障或手动复位，此接口也可用于发送从主用无线控制器到备用无线控制器的通知消息。备用无线控制器会使用此接口来和Syslog，NTP服务器和TFTP服务器通信进行配置上传。



冗余端口

这个接口在新的高可用性架构下扮演着非常重要的角色。从主用无线控制器到备用无线控制器的启动和增加批量配置就会使用这个冗余端口来进行同步。高可用性配置中的无线控制器将使用这个端口来进行高可用性角色的协商。冗余端口从备用无线控制器到主用无线控制器上每100毫秒（默认定时器）发送的UDP保持活动信息，来检查对端设备的可达性。此外，一旦机箱发生故障，主用无线控制器将通过冗余端口向备用无线控制器发送通知信息。如果没有配置NTP服务器，可以通过冗余端口来手动进行主用无线控制器到备用无线控制器上的时间同步。如果是一个独立无线控制器或者是WiSM-2上的冗余VLAN，该端口将被分配一个最后2字节是参照管理接口IP最后2字节（前2个字节总是169.254）的自动生成的IP地址。

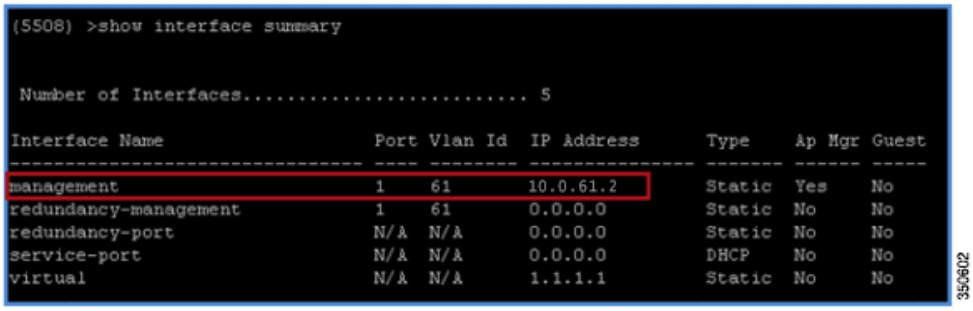


使用命令行配置高可用性

完成以下步骤：

1，在配置高可用性之前，需要保证两个无线控制器的管理接口在同一个子网中：

WLC 1:



```
(5508) >show interface summary

 Number of Interfaces.......................... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       10.0.61.2       Static  Yes    No
redundancy-management            1    61       0.0.0.0         Static  No     No
redundancy-port                  N/A  N/A      0.0.0.0         Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

350602

WLC 2:

```
(5508) >show interface summary

 Number of Interfaces.......................... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       10.0.61.3       Static  Yes    No
redundancy-management            1    61       0.0.0.0         Static  No     No
redundancy-port                  N/A  N/A      0.0.0.0         Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

350603

2，高可用性在默认情况下是不启用的。在启用高可用性之前，需要强制配置冗余管理IP地址和对端冗余管理IP地址。这两个接口应该与管理接口在同一个子网里。例如，10.0.61.21是WLC 1的冗余管理IP地址，10.0.61.23是WLC 2冗余管理IP地址。需要配置10.0.61.23 是WLC 2的冗余管理IP地址，10.0.61.21是WLC1的冗余管理IP地址。

使用命令行配置冗余和对端冗余管理IP地址：

WLC 1:

```
(5508) >config interface address redundancy-management 10.0.61.21 peer-redundancy-management 10.0.61.23

(5508) >show interface summary

 Number of Interfaces.......................... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       10.0.61.2       Static  Yes    No
redundancy-management            1    61       10.0.61.21      Static  No     No
redundancy-port                  N/A  N/A      169.254.61.21   Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      1.1.1.1         Static  No     No
```

350604

WLC 2:

```
(5508) >config interface address redundancy-management 10.0.61.23 peer-redundancy-management 10.0.61.21

(5508) >show interface summary

 Number of Interfaces.......................... 5

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
------------------------------- ---- -------- --------------- ------- ------ -----
management                       1    61       10.0.61.2       Static  Yes    No
redundancy-management            1    61       10.0.61.23      Static  No     No
redundancy-port                  N/A  N/A      169.254.61.23   Static  No     No
service-port                     N/A  N/A      0.0.0.0         DHCP    No     No
virtual                          N/A  N/A      169.254.61.23   Static  No     No
```

350937

3，在这个步骤中使用控制命令行配置一个无线控制器作为主无线控制器（默认情况下，控制器UID是HA的是主用无线控制器的，并且在上面应该安装有效的基于无线接入点的许可），另一个无线控制器作为备用无线控制器（将继承主无线控制器上的无线接入点计数许可）。在这个例子中，WLC 1被配置为主用无线控制器，WLC2被配置为备用无线控制器：

WLC 1:

```
(5508) >config redundancy unit primary

(5508) >show redundancy summary
 Redundancy Mode = SSO DISABLED
      Local State = ACTIVE
       Peer State = N/A
             Unit = Primary
          Unit ID = 00:24:97:69:D2:20
Redundancy State = N/A
     Mobility MAC = 00:24:97:69:D2:20

Redundancy Management IP Address..................10.0.61.21
Peer Redundancy Management IP Address............10.0.61.23
Redundancy Port IP Address.......................169.254.61.21
Peer Redundancy Port IP Address..................169.254.61.23
```

350605

WLC 2:

```
(5508) >config redundancy unit secondary

(5508) >show redundancy summary
 Redundancy Mode = SSO DISABLED
      Local State = ACTIVE
       Peer State = N/A
             Unit = Secondary - HA SKU
          Unit ID = 00:24:97:69:78:20
Redundancy State = N/A
     Mobility MAC = 00:24:97:69:78:20

Redundancy Management IP Address.................. 10.0.61.23
Peer Redundancy Management IP Address............ 10.0.61.21
Redundancy Port IP Address.......................  169.254.61.23
Peer Redundancy Port IP Address..................  169.254.61.21
```

350606

Note

如果是从工厂订购的7.3版本以上的HA SKU，您不需要配置备用设备。工厂订购的HA SKU是一个默认的备用设备，当和拥有无线接入点计数许可的主用无线控制器第一次一起使用时，就会自动成为备用无线控制器。

如果您希望将现有的无线控制器用作备用无线控制器，请务必使用CLI里的冗余配置命令进行配置。只有当无线控制器想要工作在备用状态，并且无线控制器上面有永久计数许可的时候，这些命令才会起作用。当5500系列控制器最少需要50个无线接入点许可时才能被转换成备用无线控制器。但是对于WiSM-2，7500/8500无线控制器就没有这样的限制。

在无线控制器上配置了冗余管理和对端冗余管理IP地址，并配置成冗余单元设备之后，就可以启用SSO功能了。一定要要确保两个无线控制器之间的物理连接是连通的（即两个无线控制器用以太网线背靠背地连接了冗余端口），并且确保无线控制器在启用SSO之前上联到了网络交换机，并且到网关的链路是可达的。

一旦启用了SSO功能，无线控制器就会重启。在启动过程中，无线控制器会通过冗余端口来协商确定它的高可用性角色。如果无线控制器不能通过冗余端口或冗余管理接口互相通信，配置为备用的无线控制器就会进入维护模式。“维护模式”在本文档后面会有讨论。

5，在这个步骤中使用命令行来启用无线接入点SSO功能。请记住，启用无线接入点SSO将会重启无线控制器。
WLC 1:

```
(5508) >config redundancy mode sso


All unsaved configuration will be saved.
And the system will be reset. Are you sure? (y/n)y


Configuration Saved!
System will now restart!
```

WLC 2:

```
(5508) >config redundancy mode sso


All unsaved configuration will be saved.
And the system will be reset. Are you sure? (y/n)y


Configuration Saved!
System will now restart!
```

6，启用SSO功能将重新启动无线控制器以便在每个配置平台上重新协商高可用性角色。当设备的角色确定后，备用无线控制器就会通过冗余端口从主用无线控制器同步配置。最初，备用无线控制器会报告XML不匹配，会从主用无线控制器上下载配置后再次重启。在高可用性角色确定后再次重新启动时，会再次验证配置，就没有XML配置不匹配的报告了，就会进行下面的流程配置使该设备成为备用无线控制器。

这是两台无线控制器上的启动日志：

WLC 1:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
```

WLC 2 启用SSO功能后的第一次启动：

```
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are different, reboot required
New XML downloaded Category: rsyncmgrXferTrasport.
Restarting system ..
Restarting system.
```

350610

Note

一旦启用了SSO功能，备用无线控制器就可以通过console线连接，通过服务端口的SSH / Telnet连接和冗余管理接口上的SSH进行连接。

WLC 2 从主用无线控制器上下载完XML配置后进行第二次重新启动

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

350611

7，启用SSO功能后，无线控制器重新启动，同步XML配置，WLC 1会转换到主用状态，WLC 2转换到热备份状态。从这时开始，WLC2上管理接口的GUI / TELNET / SSH将无法正常访问，这时所有的配置和管理应该从主用无线控制器完成。如果需要的话，备用无线控制器（在这个例子中的WLC 2）只能通过console线或通过服务端口来管理。

此外，一旦对端无线控制器转换到热备份状态，-standby关键字会自动附加到备用无线控制器的提示名称上。

```
User: Cisco
Password:*********
(5508-Standby) >
(5508-Standby) >
(5508-Standby) >
```

350612

8，完成下边的步骤检查冗余状态：

a. 对于WLC 1，进入到**Monitor > Redundancy > Summary**

```
(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 = 492 usecs
Average Management Gateway Reachability Latency = 600 usecs

Redundancy Management IP Address..................  10.0.61.21
Peer Redundancy Management IP Address............  10.0.61.23
Redundancy Port IP Address........................  169.254.61.21
Peer Redundancy Port IP Address...................  169.254.61.23
Peer Service Port IP Address..................... 0.0.0.0
```

350613

b. 对于WLC 2，使用Console口连接：

```
(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 = 481 usecs
Average Management Gateway Reachability Latency = 2603 usecs

Redundancy Management IP Address.................10.0.61.23
Peer Redundancy Management IP Address............10.0.61.21
Redundancy Port IP Address....................... 169.254.61.23
Peer Redundancy Port IP Address................... 169.254.61.21
```

350938

注意

一旦启用了 SSO，备用无线控制器可以通过console线连接，服务端口上的SSH / Telnet和冗余管理端口上的SSH来连接。

通过GUI图形界面配置高可用性

完成以下步骤：

1，在配置HA之前，会强制性的要求两个无线控制器的管理接口在同一子网中：

WLC 1:

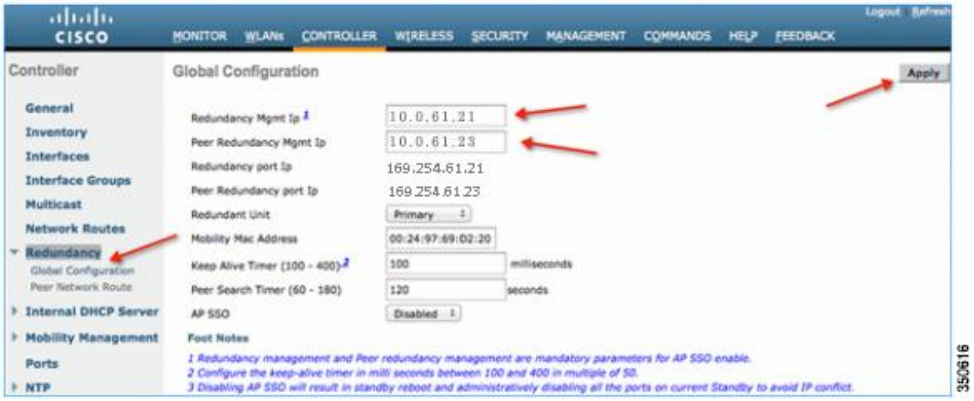
350614

WLC 2:

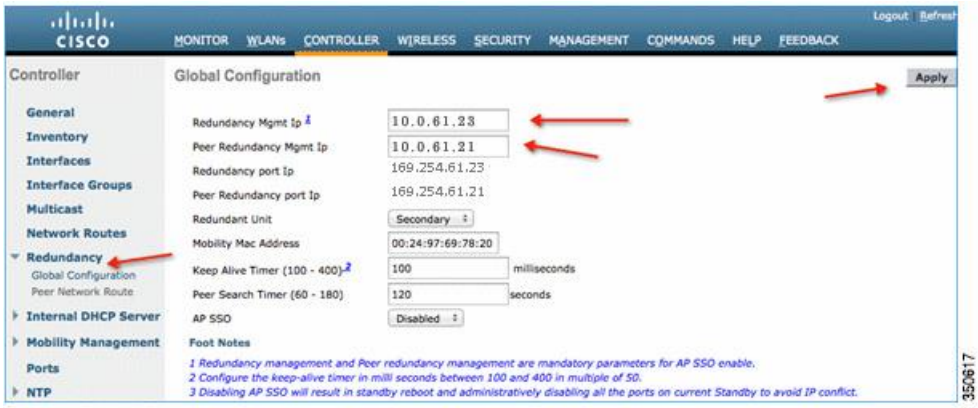
2，高可用性在默认情况下是不启用的。在您启用高可用性之前，会强制要求配置冗余管理IP地址和对端冗余管理IP地址。这两个接口应该与管理接口在同一个子网里。在这个例子中，10.0.61.21是WLC 1的冗余管理IP地址，10.0.61.23是WLC 2的冗余管理IP地址。需要在WLC 2进行配置，让10.0.61.23作为WLC 2的冗余管理IP地址，10.0.61.21作为WLC 1的冗余管理IP地址。

在这两个接口上输入IP地址，并单击“应用”。

WLC 1:



WLC 2:



3，在Redundant Unit的下拉列表里配置其中一个无线控制器作为主用无线控制器，另一台作为冗余无线控制器。在这个例子中，WLC1配置为主用，WLC 2被配置为备用。配置完成后单击应用。

WLC 1:

WLC 2:

注意

如果是从工厂订购的7.3版本以上的HA SKU，您不需要配置备用设备。工厂订购的HA SKU是一个默认的备用设备，当和实际拥有无线接入点计数许可的主用无线控制器第一次一起使用时，就会成为备用无线控制器。

如果您希望将现有的无线控制器用作备用无线控制器，请务必使用CLI里的冗余配置命令进行配置。只有当无线控制器想要工作在备用状态，并且无线控制器上面有永久计数许可的时候，这些命令才会起作用。当5500系列控制器最少需要50个无线接入点许可时才能被转换成备用无线控制器。但是对于WiSM-2，7500/8500无线控制器就没有这样的限制。

4, 在无线控制器上配置了冗余管理和对端冗余管理IP地址，并配置成冗余单元设备之后，就可以启用SSO功能了。一定要要确保两个无线控制器之间的物理连接是连通的（即两个无线控制器用以太网线背靠背地连接了冗余端口），并且确保无线控制器在启用SSO之前上联到了网络交换机，并且到网关的链路是可达的。

一旦启用了SSO功能，无线控制器就会重启。在启动过程中，无线控制器会通过冗余端口来协商确定它的高可用性角色。如果无线控制器不能通过冗余端口或冗余管理接口互相通信，配置为备用的无线控制器就会进入维护模式。“维护模式”在本文档后面会有讨论。

5, 为了要启用AP SSO功能，在两台无线控制器上的下拉列表中选择“启用”，然后点击“应用”。在启用了AP SSO功能之后，无线控制器会重新启动，并把默认信息填在其他选项中，如对等服务端口的IP，对等冗余端口的IP等等。

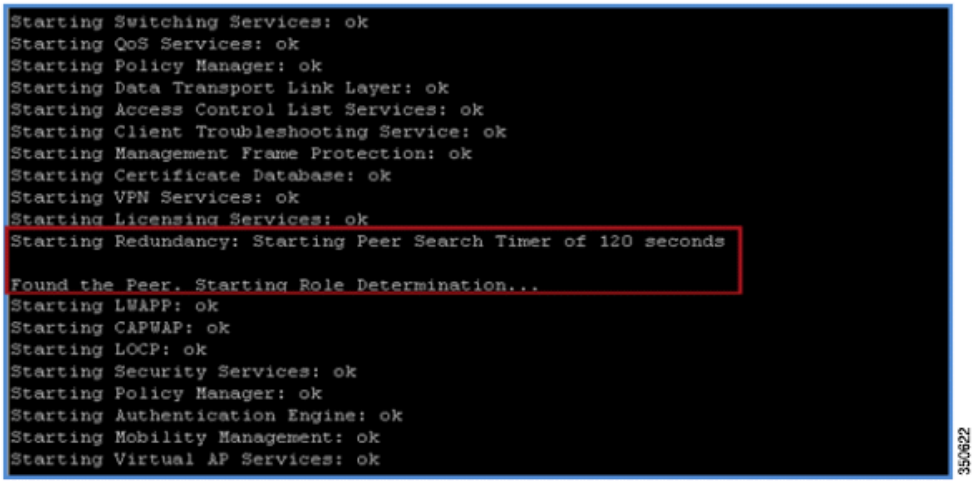
WLC 1:

WLC 2:

6， 启用SSO功能将重新启动无线控制器以便在每个配置平台上重新协商高可用性角色。当设备的角色确定后，备用无线控制器就会通过冗余端口从主用无线控制器同步配置。最初，备用无线控制器会报告XML不匹配，会从主用无线控制器上下载配置后再次重启。在高可用性角色确定后再次重新启动时，会再次验证配置，就没有XML配置不匹配的报告了，就会进行下面的流程配置使该设备成为备用无线控制器。

以下是无线控制器的启动日志信息：

WLC 1:



在启用SSO功能后WLC第一次重启

```
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are different, reboot required
New XML downloaded Category: rsyncmgrXferTrasport.
Restarting system ..
Restarting system.
```

350623

注意

一旦启用了SSO，备用无线控制器可以通过console线连接，服务端口上的SSH / Telnet，冗余管理端口上的SSH连接。

WLC2从主无线控制器上下载了XML配置后，进行第二次启动:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

350624

7. 启用SSO后，无线控制器重新启动并同步XML配置，WLC 1转化为主用状态和WLC 2转化为热备份状态状态。从这时开始，WLC2上管理接口的GUI / TELNET / SSH 将无法正常工作，所有的配置和管理应该从主用无线控制器完成。如果需要的话，备用无线控制器（在里是WLC 2）只能通过服务端口或console线来管理。

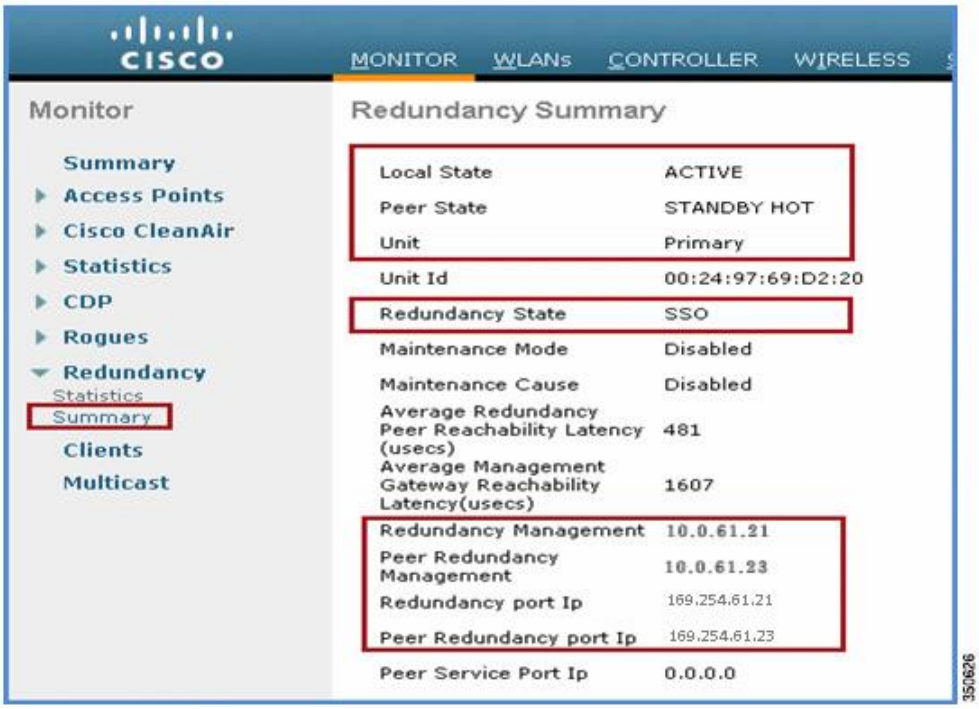
此外，一旦对端的无线控制器转换到热备份状态，-standby关键字会自动附加到备用无线控制器的提示名称上。

```
User: Cisco
Password:*********
(5508-Standby) >
(5508-Standby) >
(5508-Standby) >
```

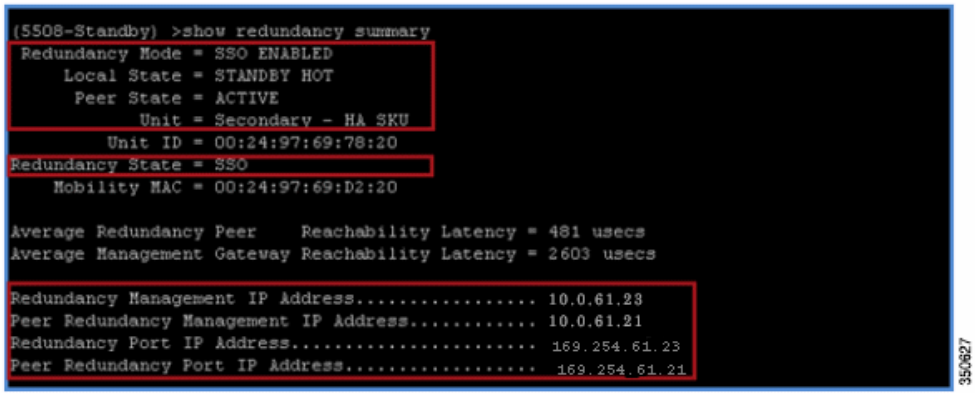
350625

8. 完成以下步骤检查冗余状态：

   a. 对于WLC 1，进入Monitor > Redundancy > Summary页面：



b. 对于WLC 2，进入到Console控制台连接：



注意

一旦启用了SSO，备用无线控制器可以通过console连接，服务端口的SSH / Telnet连接，冗余管理端口的SSH连接。

通过配置向导配置高可用性

完成以下步骤：

1， 两个无线控制器之间的HA也可以通过配置向导启用。它强制要求双方无线控制器上配置的管理IP地址在同一个子网中，然后再启用高可用性。

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: 10.0.61.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.0.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.0.0.100
```

350628

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: 10.0.61.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.0.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.0.0.100
```

350629

2，配置管理IP后，向导会提示您是否启用高可用性。输入yes启用高可用性，其次输入主/备单元和冗余管理以及对等管理IP地址的配置。

- 在这个例子中，WLC 1被配置作为主用无线控制器，并将作为活动的无线控制器。WLC 2配置为辅助，并承担备用的无线控制器的角色。
- 在输入主/备单元后，会强制性要求配置冗余管理和对等冗余管理IP地址。这两个接口应该与管理接口在同一个子网中。在这个例子中，10.0.61.21是WLC 1的是冗余管理IP地址，10.0.61.23是WLC 2的冗余管理IP地址。需要在WLC 2配置冗余管理IP地址为10.0.61.23，相应的在WLC1中配置冗余管理IP地址为10.0.61.21。

  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: 10.0.61.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.0.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.0.0.100

Enable HA [yes][NO]: yes

Configure HA Unit [PRIMARY][secondary]: Primary

Redundancy Management IP Address: 10.0.61.21

Peer Redundancy Management IP Address: 10.0.61.23

Virtual Gateway IP Address: 1.1.1.1
```

350630

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: 10.0.61.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.0.61.1
Management Interface VLAN Identifier (0 = untagged): 61
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.0.0.100

Enable HA [yes][NO]: yes

Configure HA Unit [PRIMARY][secondary]: secondary

Redundancy Management IP Address: 10.0.61.23

Peer Redundancy Management IP Address:10.0.61.21

Virtual Gateway IP Address: 1.1.1.1
```

350631

3，在配置向导中启用高可用性后，继续配置这些参数：

- 虚拟IP地址
- 移动域名称
- SSID
- DHCP桥接模式
- RADIUS配置
- 国家代码
- NTP配置等等

在保存了配置之后无线控制器将会重新启动。

4. 在启动时无线控制器将协商高可用性的角色。在确定角色之后，主用无线控制器将通过冗余端口向备用无线控制器同步配置。在最开始配置了无线控制器之后，备用无线控制器将报告XML配置不匹配，会从主用无线控制器下载配置后再重新启动。在角色确定并重启后将再次验证配置，报告没有XML配置不匹配，将本身作为备用无线控制器。

下面是无线控制器上的启动日志：

WLC 1:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
```

350632

WLC 2在启用高可用性之后重新启动：

```
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...

config interface address management 10.0.61.2 255.255.255.0 10.0.61.1
config interface address service-port 10.10.10.10 255.255.255.0
config coredump enable
config interface address management 10.0.61.3 255.255.255.0 10.0.61.1
config interface address service-port 10.10.10.11 255.255.255.0

Startup XMLs are different, reboot required
New XML downloaded Category: rsyncmgrXferTrasport.
Restarting system ..
Restarting system.
```

350633

WLC2从主用无线控制器中下载XML配置后第二此重启：

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

350634

注意

一旦启用了SSO，备用无线控制器可以通过控制台，SSH / Telnet的服务端口，SSH的冗余管理接口上进行连接。

5. 在启用了高可用性，无线控制器重新启动以及XML配置同步后，WLC 1要将其状态更改为活动，WLC2转换其状态为热备。从这时开始WLC2的Telnet/SSH/GUI管理界面将无法工作，所有的配置和管理应该从主用无线控制器进行。如果需要的话，备用无线控制器（在此例中为WLC 2）只能在控制台或服务端口来管理。

此外，一旦对等的无线控制器转换到热备状态，-Standby关键字将自动追加到备用无线控制器的提示名称。

```
User: Cisco
Password:*********
(5508-Standby) >
(5508-Standby) >
(5508-Standby) >
```

350635

6，完成以下这些步骤检查冗余状态：

a. 对于WLC 1

```
(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................... 10.0.61.21
Peer Redundancy Management IP Address............... 10.0.61.23
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
```

350636

b. 对于WLC 2，进入到Console控制台连接

```
(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................ 10.0.61.23
Peer Redundancy Management IP Address........... 10.0.61.21
Redundancy Port IP Address...................... 169.254.61.23
Peer Redundancy Port IP Address................. 169.254.61.21
```

350637

注意

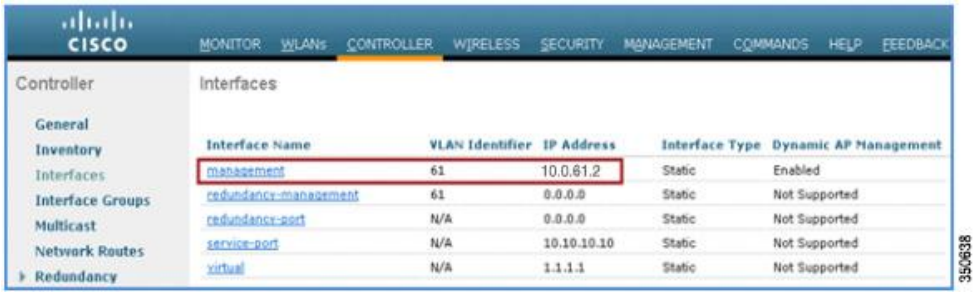
一旦启用了SSO，备用无线控制器可以通过控制台连接，SSH / Telnet的服务端口，冗余管理接口上的SSH连接。

通过Cisco Prime配置高可用性

完成以下步骤：

1. 在配置HA之前，需要将两个无线控制器的管理接口配置在同一子网内，这是强制性的。

   WLC 1:

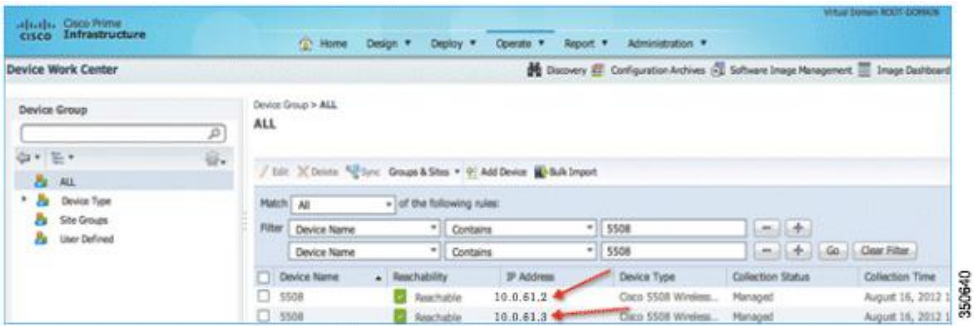


350638

   WLC 2:

350639

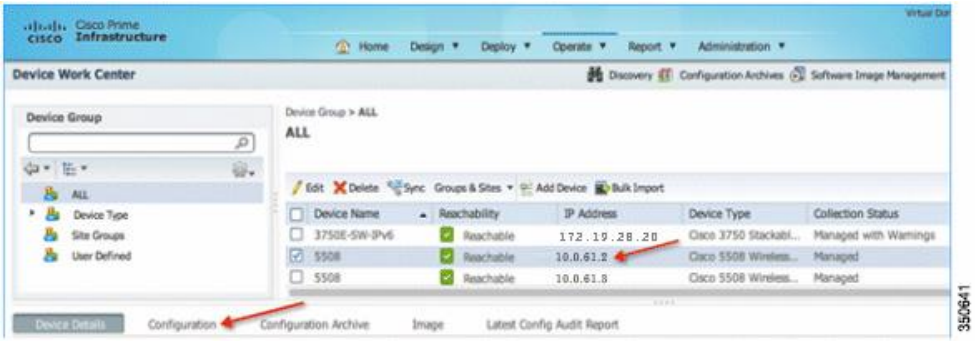
2. 在Cisco Prime中使用各自的管理IP地址来添加两个无线控制器。一旦添加成功，就可以在Operate > Device Work Center页面下查看。



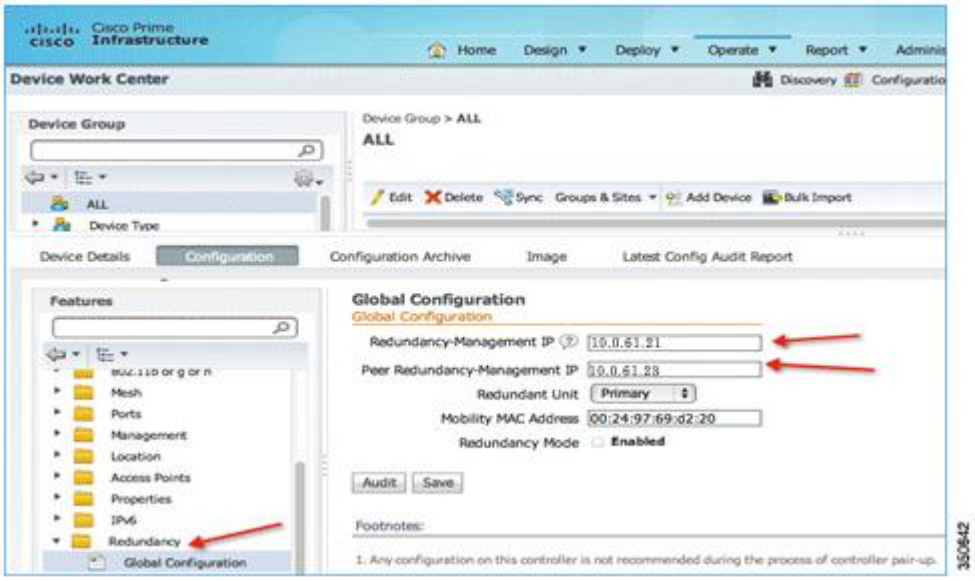
3. 高可用性在默认情况下是禁用的。在您启用高可用性之前，需要强制性的配置冗余管理IP地址的和对等冗余管理IP地址。这两个接口应该与管理接口在同一个子网中。在这个例子中，10.0.61.21是WLC 1冗余管理IP地址，10.0.61.23是WLC 2冗余管理IP地址。需要在WLC 2中配置冗余管理IP地址为10.0.61.23，相应的在WLC 1中配置冗余管理IP地址为10.0.61.21。

为了从Cisco Prime中进行配置，需要进入Operate > Device Work Center界面，在需要配置高可用性的无线控制器前边的单选框上点击。一旦选中，单击“配置”选项卡，它提供了配置WLC 1所需要的所有选项，重复这些步骤可以对WLC 2进行配置。

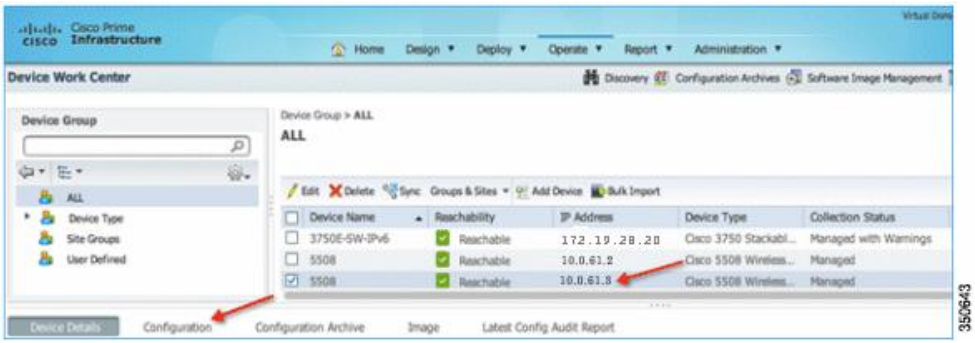
WLC 1:



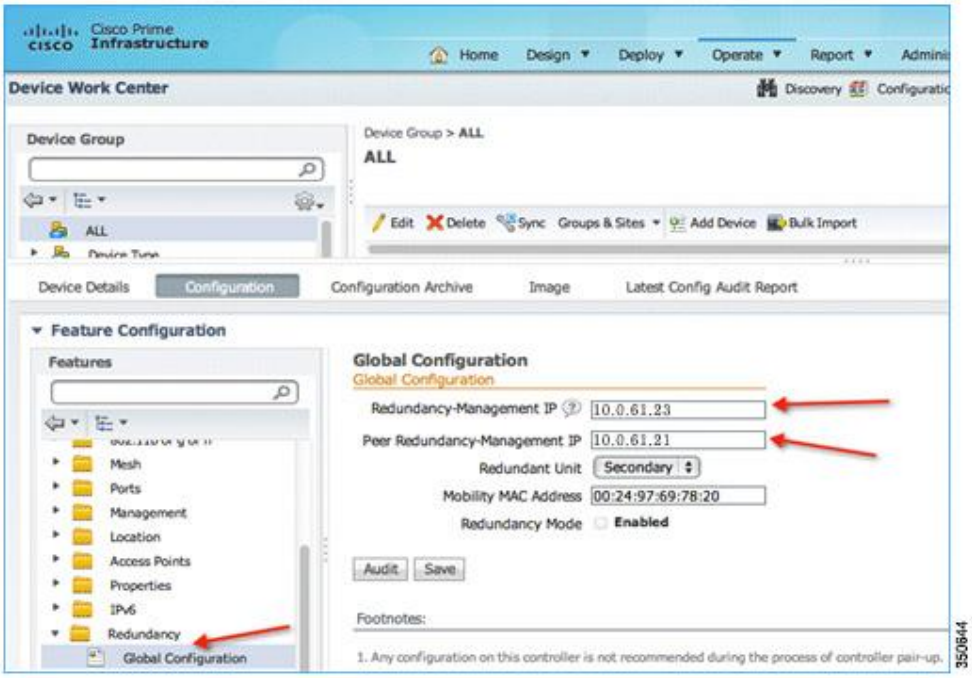
为了配置WLC 1的高可用性参数，进入到Redundancy > Global Configuration界面，输入冗余和对等冗余管理IP地址，然后单击“保存”。



WLC 2:

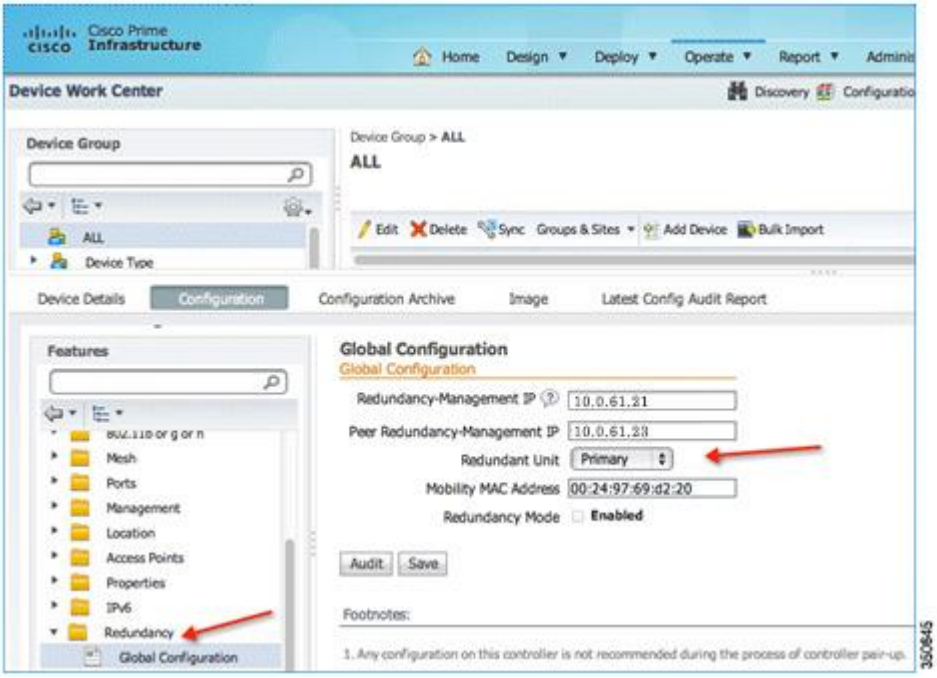


为了配置WLC 2的高可用性参数，进入到Redundancy > Global Configuration界面，输入冗余和对等冗余管理IP地址，然后单击“保存”。

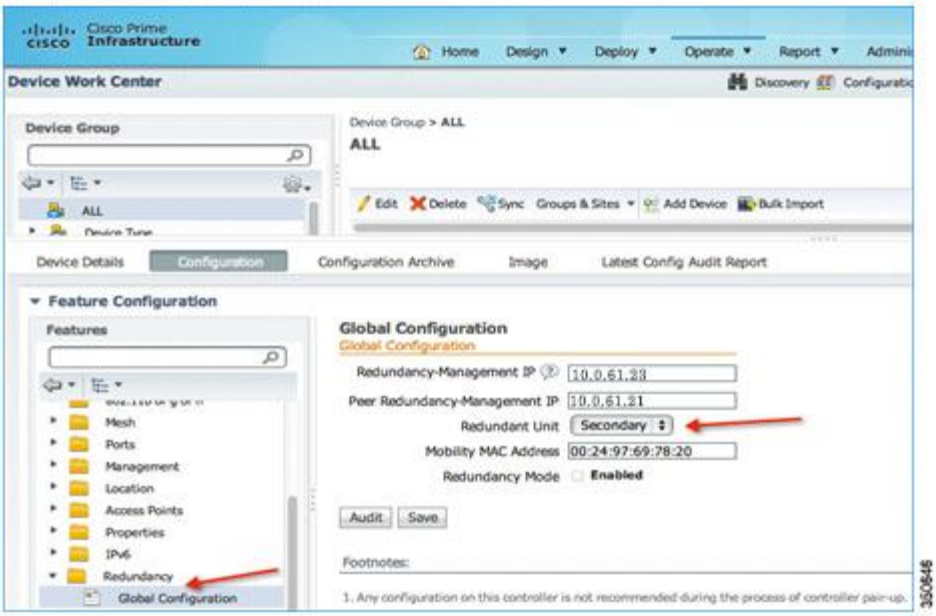


4. 从冗余下拉列表中将一个无线控制器配置为主用无线控制器，另外一个配置为备用无线控制器。在这个例子中，WLC 1配置为主用和WLC 2被配置备用。配置完成后，单击“保存”。

WLC 1:



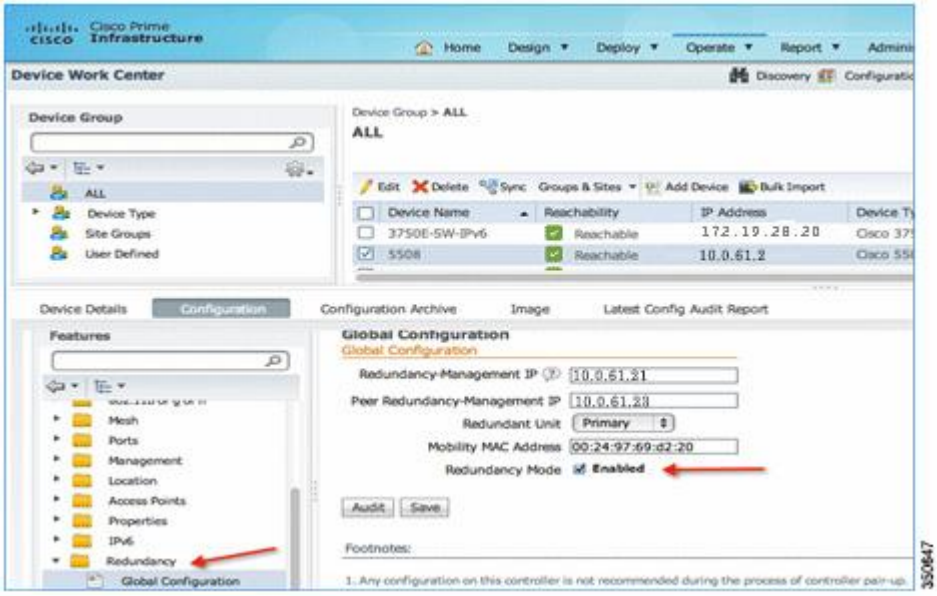
WLC 2:



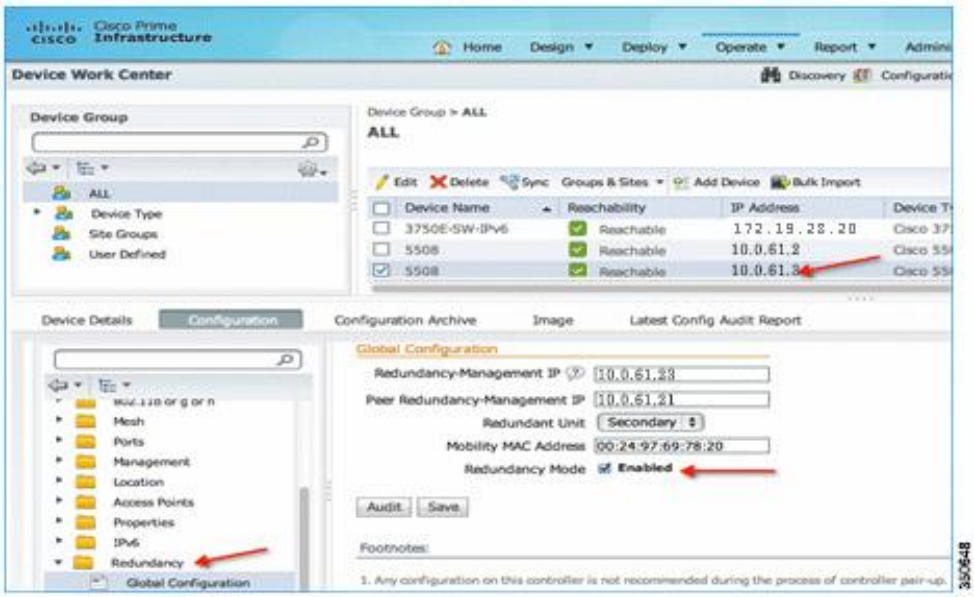
5.在无线控制器上配置冗余管理、对等冗余管理IP地址和冗余单元之后，然后就该配置SSO功能了。一旦启用了SSO，无线控制器就会重新启动。在启动时，无线控制器会通过冗余端口对HA角色进行协商。如果无线控制器上不能通过冗余端口或通过冗余管理接口与对方通信，被配置为备用的无线控制器将进入维护模式。“维护模式”在本文档后面进行了讨论。

6. 选择“启用”复选框以启用冗余模式，然后单击“保存”。在冗余模式启用后，无线控制器将重新启动。

WLC 1:



WLC 2:



7. 启用SSO将重新启动无线控制器来协商HA角色。确定角色后，配置通过冗余端口从主用无线控制器同步到备用无线控制器。最初无线控制器被配置后，作为备份的无线控制器会报告XML配置不匹配，然后会从主用无线控制器下载配置，再次重新启动。在无线控制器角色确定后，在下次重新启动时，它会再次验证配置，报告没有XML配置不匹配，以进一步建立本身作为备用无线控制器。

以下是两个无线控制器的启动日志：

WLC 1:

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
Starting Mobility Management: ok
Starting Virtual AP Services: ok
```

350649

在启用SSO后WLC2第一次重新启动：

```
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are different, reboot required
New XML downloaded Category: rsyncmgrXferTrasport.
Restarting system ..
Restarting system.
```

350650

注意

一旦启用了SSO，备用无线控制器可以通过控制台连接，SSH / Telnet的服务端口连接，SSH的冗余管理界面连接。

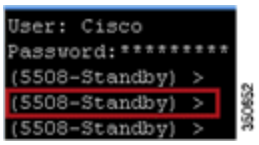
从主用无线控制器下载XML配置后，WLC 2第二次重新启动：

```
Starting Switching Services: ok
Starting QoS Services: ok
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
Starting LOCP: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

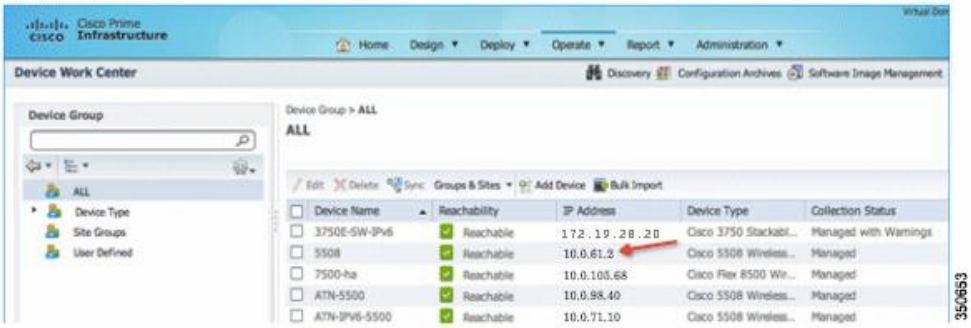
350651

8.在SSO启用后无线控制器重新启动并且同步XML配置，WLC1进入活动状态，WLC 2将进入热备份状态。从这时开始，WLC2管理接口的GUI/TELNET/SSH将无法正常工作，应该从主用无线控制器进行所有的配置和管理。如果需要的话，备用无线控制器（在这个例子里是WLC 2）只能通过控制台或服务端口来管理。

此外，一旦对等的无线控制器转换到备用的热状态，-Standby关键字将自动追加到备用无线控制器的提示名称。



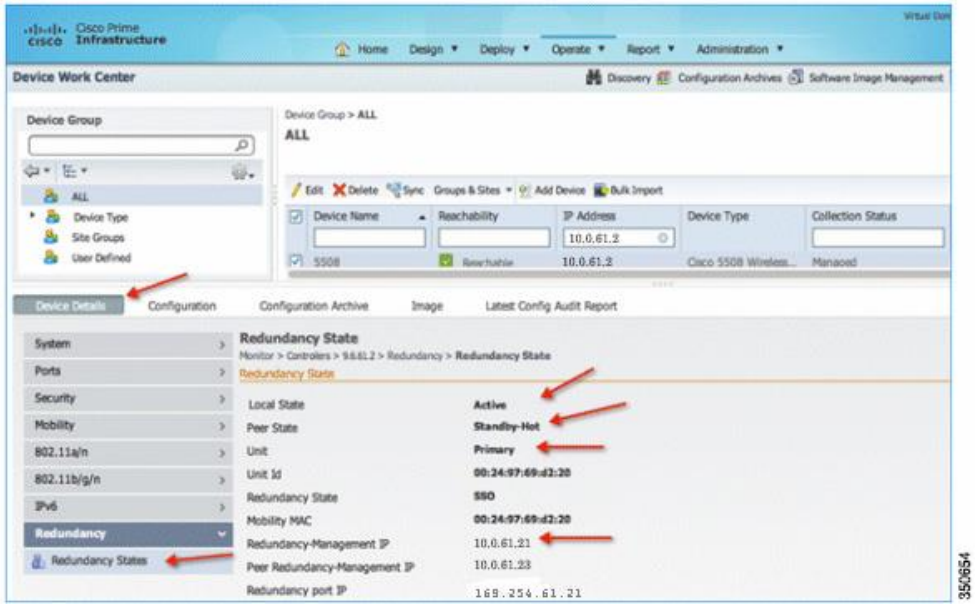
9. 一旦高可用性配对形成，Cisco Prime会从它的数据库中移除/删除WLC 2的入口，因为两个无线控制器上有相同的管理IP地址。对于网络而言，他们成为一个活动的无线控制器。



注意

从图像中看到只有WLC 1（IP地址配置为10.0.61.2作为主用单元）在Cisco Prime上是活跃的。WLC 2最初添加IP地址10.0.61.3到Cisco Prime上，高可用性配对形成后，WLC 2会从Cisco Prime数据库中删除掉。

10.为了检查主用无线控制器的冗余状态，进入到Cisco Prime中的Device Details > Redundancy > Redundancy States界面。



升级高可用性配置中的无线控制器

备用无线控制器不能从TFTP/FTP服务器直接升级。所有的脚本执行完毕后，主用无线控制器传输软件镜像到备用无线控制器。一旦备用无线控制器从主用无线控制器接收到软件镜像，它开始执行升级脚本。可以在主用无线控制器上查看到备用无线控制器的镜像传输和脚本执行的所有日志。

```
(5508) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Code
TFTP Server IP........................................... 10.0.0.100
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path.................................................
TFTP Filename............................................ AS_5500_7_3_1_47.aes

This may take some time.
Are you sure you want to start? (y/N) y

TFTP Code transfer starting.

TFTP receive complete... extracting components.

Checking Version Built.

Image version check passed.

Writing new RTOS to flash disk.

Writing new FP to flash disk.

Writing new APIB to flash disk.

Executing install_apib script.

Executing fini script.

TFTP File transfer successful on Active Controller

Transferring file to the Standby Controller

Standby - Standby receive complete... extracting components.

Standby - Checking Version Built.

Standby - Image version check passed.

Standby - Writing new RTOS to flash disk.

Standby - Writing new FP to flash disk.

Standby - Writing new APIB to flash disk.

Standby - Executing install_apib script.

Standby - Executing fini script.

Standby - Standby File transfer is successful.

Reboot the controller for update to complete.
Optionally, pre-download the image to APs before rebooting to reduce network downtime.

(5508) >
```

350655

高可用性配置中的升级步骤

完成以下步骤：

1. 在无线控制器上配置HA后，备用无线控制器不能直接从TFTP/FTP服务器升级。
2. 通过CLI/GUI在主用无线控制器上启用升级，并等待升级完成。
3. 一旦主用无线控制器执行所有的升级脚本，它会通过冗余端口将整个镜像传输到备用无线控制器。
4. 当备用无线控制器从主用无线控制器接收到的镜像，它就会开始执行升级程序。备用无线控制器可以通过主用无线控制器的Console/Telnet/SSH/HTTP连接查看脚本的执行情况。
5. 备用无线控制器升级成功后的消息一旦在主无线控制器上观察到，在主用无线控制器上利用show boot命令确定新镜像作为主镜像是非常重要的。
6. 验证完成后，在主用无线控制器上初始化主镜像以传输新的镜像到网络中的所有无线接入点。
7. 所有的无线接入点的镜像完成升级后，发出show ap image all命令确认无线控制器的主镜像被设置为无线接入点上的备用镜像。
8. 启动交换选项在无线接入点上交换备用镜像为主镜像。此实现中，无线控制器和无线接入点的主镜像都更换为新镜像。
9. 利用schedule-reset命令作为“no swap option”选项以重置无线接入点和无线控制器，使他们可以启动新镜像。
10. 备用无线控制器将会在计划重置时间的一分钟之前重启，并采用新镜像在网络中启动。
11. 所有的无线接入点将重新启动，并加入新的主用无线控制器，之前的主用无线控制器将过渡到备用状态。
12. 使用show boot，show sysinfo，show ap image all和show redundancy summary命令确定两个无线控制器和无线接入点采用新镜像启动。

启动高可用性配置的无线控制器升级之前的重要指南

- 此版本中不支持服务升级，所以HA配置下升级无线控制器应规划网络故障停机时间。
- 在开始升级HA配置的无线控制器之前，对等无线控制器应该是处在热备状态。
- 建议在升级后同时重新启动无线控制器以防软件版本不匹配。
- 计划重启适用于HA设置的无线控制器。对等无线控制器在主用无线控制器的计划定时器到期的前一分钟重新启动。
- 如果没有设置计划重启，可以从主用无线控制器上通过使用reset peer-system命令重启备用无线控制器。
- Debug transfer命令的可以在主用无线控制器或者备用无线控制器上启用。

高可用性设置的下载/上传事项

- 备用无线控制器不能直接下载和上传配置。
- 所有下载的文件类型，如镜像，配置，Web认证包和签名文件将被在主用无线控制器上下载，然后自动推送到备用无线控制器。
- 在主用无线控制器的配置文件一旦被下载，它将被推到备用无线控制器。这将导致首先重启备用无线控制器，随之重启主用无线控制器。
- 对等的服务端口和静态路由的配置是不同的XML文件的一部分，如果下载内容作为配置文件的一部分，XML文件将不会被申请。
- 证书的下载应该在每个机箱各自下载，并且需要在配对前完成。
- 上传不同的文件类型，如配置，事件日志，崩溃文件等可以从备用无线控制器单独完成。然而，CLI来配置不同的上传参数如服务器IP，文件类型，路径和名称等需要在主用无线控制器上配配置。一旦上传参数在主用无线控制器配置，transfer upload peer-start命令应在主用无线控制器上使用，初始化备用无线控制器的加载。
- 服务端口的状态将从主用无线控制器同步化到备用无线控制器。也就是说，如果在主用无线控制器服务端口启用了DHCP，备用无线控制器也将使用DHCP获得的服务端口IP地址。如果该主用无线控制器的服务端口配置一个静态的IP地址，备用无线控制器也需要配置不同的静态IP地址。用来配置备用无线控制器服务端口的IP地址的CLI是configure redundancy interface address peer-service-port <IP Address >。应该从主用无线控制器执行此命令。此外，为了在备用无线控制器的带外管理的服务端口配置路由，在主用无线控制器使用configure redundancy peer-route add <Network IP Address ><IP Mask><Gateway>命令。

高可用性配置的切换过程

在HA配置中，无线接入点的CAPWAP状态保持在主用无线控制器和备用无线控制器（仅为在运行状态下的无线接入点）。也就是说，运行时间和关联运行时间是维护在两个无线控制器的，当启动了切换时，备用无线控制器接管网络。在这个例子中，WLC1是处于活动状态对网络进行服务，WLC2是在备用状态并在监测主用无线控制器。虽然WLC2处于备用状态，它仍然为无线接入点保持着CAPWAP状态。

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

无线控制器上高可用性配置的故障切换可分为两个不同的部分：

机箱故障切换

机箱故障切换的情况下（也就是说主用无线控制器崩溃/系统挂起/手动复位/人力切换），通过冗余端口或者冗余管理接口从主用无线控制器发送直接命令到备用无线控制器接管网络。根据网络中的无线接入点的数目，这可能要花费5-100毫秒。电源故障的情况下，主用无线控制器或不能发送一些直接命令进行切换，可能需要350-500毫秒，也取决于在网络中的无线接入点数量。

电源故障的情况下故障切换所花费的时间也取决于无线控制器配置的保持连接定时器（默认情况下，配置为100毫秒）。这里列出决定故障切换时间的算法：

- 备用无线控制器默认每100毫秒发送一次保持活动信息到主用无线控制器。发送间隔可以被配置为100-400毫秒。
- 如果在100毫秒内没有确认保持活动信号，备用无线控制器立即通过冗余管理接口发送一个ICMP消息到主用无线控制器，以检查它是否是机箱故障或冗余端口连接出现问题。
- 如果没有响应的ICMP消息，备用无线控制器立即发送另一个keep alive消息，并将等待应答的时间减少25％（即75毫秒或100毫秒减少25％）。
- 如果在75毫秒没有确认的活，备用无线控制器立即通过冗余管理接口发送另一个ICMP消息到主用无线控制器。
- 同样，如果没有第二ICMP 消息的响应，备用无线控制器变得更积极，并立即从备用无线控制器发送另一个keep alive消息，并将等待应答的时间减少25％（即，50毫秒或最后保持活定时器75毫秒 - 100毫秒的减少25％）。
- 如果没有在50毫秒内确认的第三个keep alive数据包，备用无线控制器立即通过冗余管理接口发送另一个ICMP消息到主用无线控制器。
- 最后，如果没有第三个ICMP数据包的响应，备用无线控制器宣布主用无线控制器死亡，承担主用无线控制器的角色。

网络故障切换

在网络故障切换的情况下（也就是，在主用无线控制器由于某种原因无法到达其网关），根据在网络中的无线接入点的数目，完整的切换时间可能需要3-4秒。

模拟机箱切换的步骤：

完成以下步骤：

1. 根据配置章节里的解释完成这些步骤，使得在两个无线控制器之间配置HA，并且确保手动启动切换之前，两个无线控制器配对成主用无线控制器和备用无线控制器。

   WLC 1:

```
(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................... 10.0.61.21
Peer Redundancy Management IP Address............... 10.0.61.23
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:

```
(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................... 10.0.61.23
Peer Redundancy Management IP Address............... 10.0.61.21
Redundancy Port IP Address......................... 169.254.61.23
Peer Redundancy Port IP Address.................... 169.254.61.21
```

2. 将无线接入点关联到无线控制器并在两个无线控制器上检查无线接入点的状态。在高可用性设置中，无线接入点数据库的镜像副本保存在两个无线控制器上。也就是说，无线接入点（仅适用于处于运行状态的无线接入点）的CAPWAP状态保持在主用无线控制器和备用无线控制器上，当切换启动，备用无线控制器接管网络。在这个例子中，WLC 1是一个主用无线控制器，WLC 2是备用无线控制器，无线接入点数据库保持在两个无线控制器上。

   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                    1                  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
```

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                    1                  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. 创建一个开放的WLAN并且关联一个客户端。客户端数据库同步到备用无线控制器上，因此客户端条目将会保存在备用无线控制器。一旦WLAN在主用无线控制器上创建，它也将通过冗余端口被同步到备用无线控制器。

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. 在主用无线控制器上输入redundancy force-switchover命令。此命令将触发手动切换，主用无线控制器将重新启动，备用无线控制器会接管网络。

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

注意

请注意，在这个例子5508-standby变成5508的提示。因为现在这个无线控制器变成了主用无线控制器，切换无线接入点所花费的时间为1毫秒。

WLC 2:

```
(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, 06 h 13 m 07 s  0 days, 06 h 11 m 56 s
```

350666

注意查看WLC2上无线接入点的CAPWAP状态，最开始是备用无线控制器，在切换后变成主用无线控制器。无线接入点启动时间和关联时间依旧维持，并且无线接入点没有进入发现状态。

下表清楚的给出在什么条件下将触发无线控制器的切换：

网络问题					
冗余端口状态	通过冗余管理接口到对端是否可达	主用无线控制器到网关是是否可达	从备用无线控制器到网关是否可达	是否切换	结果
Up	Yes	Yes	Yes	No	无动作
Up	Yes	Yes	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Up	Yes	No	Yes	Yes	发生切换
Up	Yes	No	No	No	无动作
Up	No	Yes	Yes	No	无动作
Up	No	Yes	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Up	No	No	Yes	Yes	发生切换
Up	No	No	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式

Down	Yes	Yes	Yes	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Down	Yes	Yes	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Down	Yes	No	Yes	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Down	Yes	No	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Down	No	Yes	Yes	Yes	发生切换，可能导致网络冲突。
Down	No	Yes	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式
Down	No	No	Yes	Yes	发生切换
Down	No	No	No	No	备用无线控制器会重新启动并检查网关的可达性。如果仍然无法访问，将进入维护模式

系统问题

触发	冗余端口状态	通过冗余管理接口到对端是否可达	切换	结果
CP Crash	Yes	No	Yes	发生切换
DP Crash	Yes	No	Yes	发生切换
System Hang	Yes	No	Yes	发生切换
Manual Reset	Yes	No	Yes	发生切换
Force Switchover	Yes	No	Yes	发生切换
CP Crash	No	Yes	Yes	发生切换
DP Crash	No	Yes	Yes	发生切换
System Hang	No	Yes	Yes	发生切换

Manual Reset	No	Yes	Yes	发生切换
Force Switchover	No	Yes	Yes	发生切换
CP Crash	No	No	Yes	网络问题部分更新
DP Crash	No	No	Yes	网络问题部分更新
System Hang	No	No	Yes	网络问题部分更新
Manual Reset	No	No	Yes	网络问题部分更新
Force Switchover	No	No	Yes	网络问题部分更新

高可用性的事实

- 只有在相同硬件和软件版本之间才可以HA配对。信息不匹配可能会导致进入维护模式。在配置AP SSO之前，两个无线控制器上的虚拟IP地址应该是一样的。
- 在5500/7500/8500系列无线控制器上的主备冗余端口之间建议直接连接。
- WiSM-2应该在相同的6500机箱上，或者可以被安装在VSS配置中提供可靠的性能。
- 在做HA配置前，必须完成冗余端口和基础设施网络之间的物理连接。
- 在HA设置中，主设备的MAC应作为移动性MAC以便与另一个HA设置或独立控制器形成一个移动性对等体。您还可以灵活地配置一个自定义的MAC地址，它可以作为一个移动的MAC地址，命令为redundancy mobilitymac <custom mac address>。配置完成后，你应该使用这个MAC地址，而不是系统的MAC地址，形成移动性对等体。一旦配置完HA，这个MAC就不能变了。
- 建议您使用DHCP分配HA设置中服务端口的地址。在HA启用后，如果原先服务端口被配置为静态IP，无线控制器将失去服务端口IP地址，必须重新配置。
- 当启用了AP SSO，HA设置中的无线控制器无法以SNMP/GUI方式访问服务端口。
- 例如更改虚拟IP地址，启用secureweb模式，配置Web认证代理等等的配置需要无线控制器重启。在这种情况下，主用无线控制器的重新启动会同时引发备用无线控制器的重新启动。
- 主无线控制器上的AP SSO被禁用时，它会被推到备用无线控制器上。在重新启动后，主无线控制器上所有的端口都会变成可用，而备无线控制器上的所有端口会被禁用。
- 保持活动和对等体发现定时器应该使用默认设置，目的是为了更好的性能。
- 在主无线控制器上清除配置会导致备用无线控制器上的配置被清除。
- 当AP启用SSO时，不支持内部DHCP服务器。
- SSO不支持LSC 无线接入点。L2 MGID同步时L3 MGID数据库在SSO时被清除。

维护模式

在一些情况下，备用无线控制器可能进入维护模式，这个时候无法与网络和对等体通信：

- 通过冗余管理接口无法访问网关
- 具备HA SKU的无线控制器从来没有发现对等体
- 冗余端口失效
- 软件版本不匹配（第一个启动的无线控制器进入主模式，而另一个无线控制器进入维护模式）

```
(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................ 10.0.61.23
Peer Redundancy Management IP Address........... 10.0.61.21
Redundancy Port IP Address...................... 169.254.61.23
Peer Redundancy Port IP Address................. 169.254.61.21
```

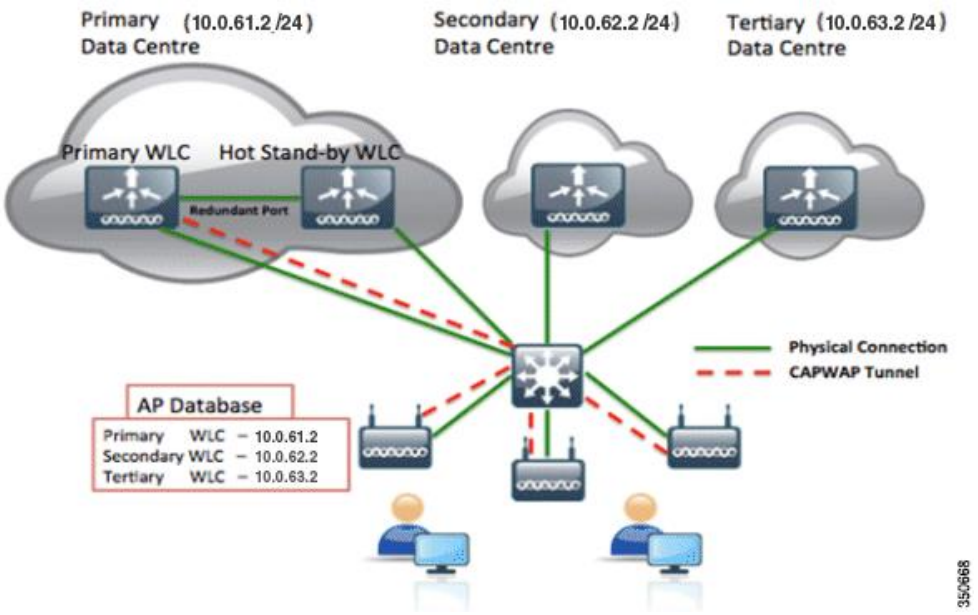
350667

注意

应该重新启动无线控制器以使其退出维护模式。在“维护模式”下只有控制台和服务端口是可用的。

传统的第一/第二/第三冗余无线控制器与高可用性SSO部署

HA（即AP SSO）可以和第二，第三控制器一起部署。在HA配置中，主用和备用无线控制器都应该被配置为首要无线控制器。仅在HA配置中的主用和备用无线控制器都出现故障的情况下，无线接入点才回退到第二和第三无线控制器。



SSO部署的移动性配置

每个无线控制器都有自己唯一的MAC地址，它和一个单独的无线控制器管理IP地址结合使用来配置移动性。在HA（即AP SSO）设置，所有无线控制器（主用和备用）都有各自唯一的MAC地址。在主设备失败，备用设备接管网络的情况下，如果主设备MAC地址在移动性设置时被使用在另一个无线控制器上，控制路径和数据路径将会失效，用户必须在移动性设置时手动在每个无线控制器上将MAC改为备用MAC地址。这是一个非常繁琐的过程，需要大量的人工干预。

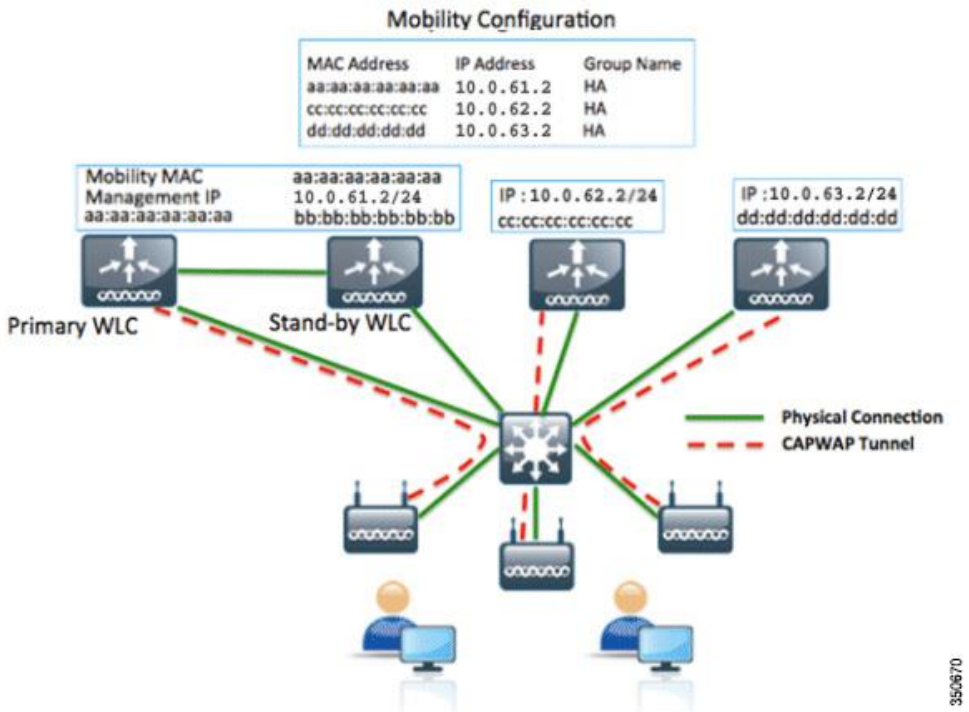
为了保持稳定的移动网络而在故障或者切换下无需人工干预，引入移动性MAC的往复（back-and-forth）概念。HA对等体被设立后，默认情况下，主用无线控制器的MAC地址与待机无线控制器的移动性MAC地址同步，可以在两个控制器上使用show redundancy summary命令查看。

```
(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................. 10.0.61.23
Peer Redundancy Management IP Address............ 10.0.61.21
Redundancy Port IP Address....................... 169.254.61.23
Peer Redundancy Port IP Address.................. 169.254.61.21
```

350669

从备用控制器的输出中可以看到移动MAC地址，它与备用无线控制器自身的MAC地址（图中Unit ID）不同。此MAC地址从主用无线控制器同步过来，并应使用在移动配置中。采用这种方式，如果主用无线控制器出现故障或即使被替换，移动MAC地址仍然可用，它会存在于备用无线控制器上，并且移动性隧道也一直可用。在更换先前主用无线控制器的情况下，新无线控制器加入到网络中，将转换其状态为备用，然后相同的移动性MAC地址会同步到新的备用无线控制器上。

您可以灵活配置自定义的MAC地址，而不是默认使用主用无线控制器MAC地址作为移动性MAC地址。可以在主无线控制器上使用configure redundancy mobilitymac <custom mac address>命令。配置完成后，你应该在其他无线控制器上使用这个MAC地址，而不是主用无线控制器MAC地址，以形成一个移动性对等体。必须先配置此MAC地址，才能形成HA对等体。一旦HA配对完成，不能修改或者编辑移动性MAC。



在这个拓扑中，主用无线控制器和备用无线控制器有自己的MAC地址。使用HA配对，主用无线控制器 MAC地址被同步为移动性MAC地址，这是在HA配对前没有配置自定义MAC的默认行为。一旦主用无线控制器的MAC地址被同步为移动MAC地址，所有控制器的移动性设置中会使用相同的MAC。

高可用性配对的授权许可

HA配对可以使用以下两个无线控制器的组合：

- 一台无线控制器具备有效的无线接入点许可证，另一台无线控制器具有HA SKU UDI
- 两台无线控制器上都有有效的无线接入点数量许可证
- 一台无线控制器有评估许可证，另一台无线控制器有HA SKU UDI或永久许可证

一台无线控制器具备有效的无线接入点许可证，另一台无线控制器具有HA SKU UDI

- HA SKU是一个新的SKU，其中无线接入点授权许可数量为0。
- HA SKU设备在启动时就是备用状态。
- 无线接入点计数许可证信息将从主设备推送到备用设备。
- 在主设备出现故障情况下，HA SKU会让一定数量的无线接入点加入，并且开启90天倒计时。粒度以天计算。
- 90天之后开始显示报警信息。但是它不会断开连接的无线接入点。
- 当新无线控制器加入后，HA SKU在配对的时候会得到无线接入点许可数

量：

- 如果新无线控制器比之前无线控制器具有更高的无线接入点数量，90天的计数器将被重置。
- 如果新无线控制器比之前无线控制器具有更少的无线接入点数量，90天的计数器将不会重置。
- 为了降低切换后的无线接入点数量，在过期之后，无线控制器偏移定时器将继续显示报警信息。

- 重启不会影响运行时间和无线接入点许可数量。
- 出厂默认下HA-SKU无线控制器不允许任何无线接入点加入。

两台无线控制器上都有有效的无线接入点数量许可证

- 应该使用CLI配置一台无线控制器为备用无线控制器（在配置章节中提到的），它要求满足最低的永久许可证数量。对于WLC5500无线控制器，需要至少50个AP永久许可才能被设置成备用无线控制器。对于WiSM-2，7500和8500就没有限制。
- 无线接入点数量许可证信息将从主设备推送到备用设备。
- 在切换发生后，新的主用无线控制器将以之前无线控制器许可证的数量工作，并开始90天的倒计时。
- 配置为备用的无线控制器不会使用它自己的安装许可证，将利用从主用无线控制器继承来的许可证。
- 90天之后，开始显示报警信息。它不会断开连接的无线接入点。
- 当新无线控制器加入后，HA SKU在配对的时候会得到无线接入点许可数量：
  - 如果新无线控制器比之前无线控制器具有更高的无线接入点数量，90天的计数器将被重置。
  - 如果新无线控制器比之前无线控制器具有更少的无线接入点数量，90天的计数器将不会重置。
  - 在切换到低的无线接入点许可数量的许可证后，在过期之后，无线控制器偏移定时器将继续显示报警信息。

一台无线控制器有评估许可证，另一台无线控制器有HA SKU UDI或永久许可证

- HA SKU设备在与现有的运行评估许可证的主用无线控制器配对时变成为备用无线控制器。或者，任何运行永久许可证的无线控制器可以使用CLI配置为备用设备，前提是满足最低永久许可证数。对于WLC5500无线控制器，需要至少50个AP永久许可才能被设置成备用无线控制器。对于WiSM-2，7500和8500就没有限制。
- 无线接入点数量许可证信息将从主设备推送到备用设备。
- 在切换发生后，新的主用无线控制器将以之前无线控制器许可证的数量工作，并开始90天的倒计时。
- 90天之后，开始显示报警信息。它不会断开连接的无线接入点。
- 当新无线控制器加入后，HA SKU在配对的时候会得到无线接入点许可数量：
  - 如果新无线控制器比之前无线控制器具有更高的无线接入点数量，90天的计数器将被重置。
  - 如果新无线控制器比之前无线控制器具有更少的无线接入点数量，90天的计数器将不会重置。
  - 在切换到低无线接入点许可数量的许可证后，在过期之后，无线控制器偏移定时器将继续显示报警信息。

7.5版本的高可用性配置

7.5版本中的冗余端口连接

- 在无线控制器版本7.3和7.4中，通过冗余端口的背对背连接，禁止了主用和备用控制器在不同的位置。有两个强制性的接口冗余，冗余端口和冗余管理接口。冗余端口使用专用的物理端口eth1(类似于服务端口)。它是用于所有冗余通信(AP、客户数据、配置同步，保持消息和角色谈判消息)。冗余管理接口是用来检查对等体和管理网关的可达性的。
- 为了支持主用和备用无线控制器能位于不同的数据中心，在版本7.5中，节点之间的背靠背的冗余端口连接不再是强制的，冗余端口可以通过交换机连接，只要两个控制器之间是L2邻接。
- 向后兼容性支持版本7.3/7.4，其中背靠背的冗余端口连接是用于无线控制器间的冗余通信，冗余管理接口用于检查对等体和管理网关的可达性。
- 冗余端口没有额外的配置更改需要，与7.3/7.4版中的配置相同。

支持的高可用性拓扑

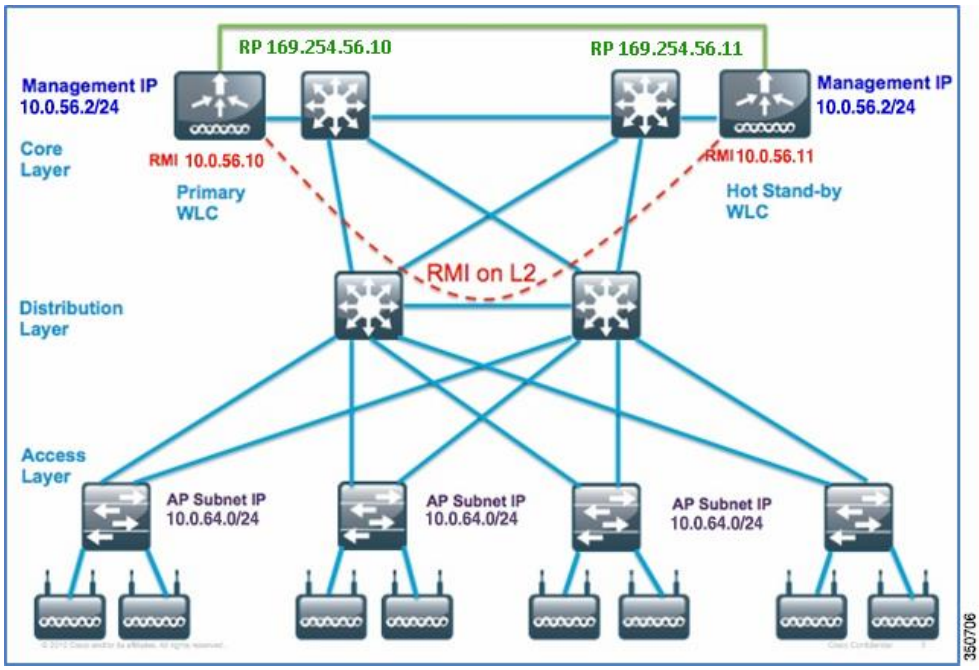
7.5版本中支持的高可用性拓扑

5500/7500/8500系列无线控制器

1. 两个无线控制器间的背靠背的冗余端口(RP)连接，冗余管理接口(RMI)检查对等体和管理网关的可达性。
2. 两个无线控制器间的RP冗余端口的2层邻接，冗余管理接口RMI检查对等体和管理网关的可达性。这可以让两个无线控制器在不同的数据中心。
3. 两个5508、7500或8500连接到一个VSS对。主用无线控制器连接到一个6500，备用无线控制器连接另一个6500。

背靠背的RP冗余端口连接

图1 背靠背的RP冗余端口连接



- 这与无线控制器7.3版本中支持的拓扑一样。
- 配置同步和Keepalive消息是通过冗余端口发送的。
- RMI冗余管理接口作为管理子网的的一部分而创建，用于检查对等体和管理网关可达性。
- 默认情况下RTT延迟为80毫秒。RTT应该为keep alive计时器的80%，keep alive可配置的范围在100 - 400毫秒。
- 故障检测时间是3 * 100 = 300 + 60 = 360 + 抖动(12毫秒)= ~ 400毫秒。
- 带宽：60Mbpd 或更多
- MTU: 1500

配置主用无线控制器：

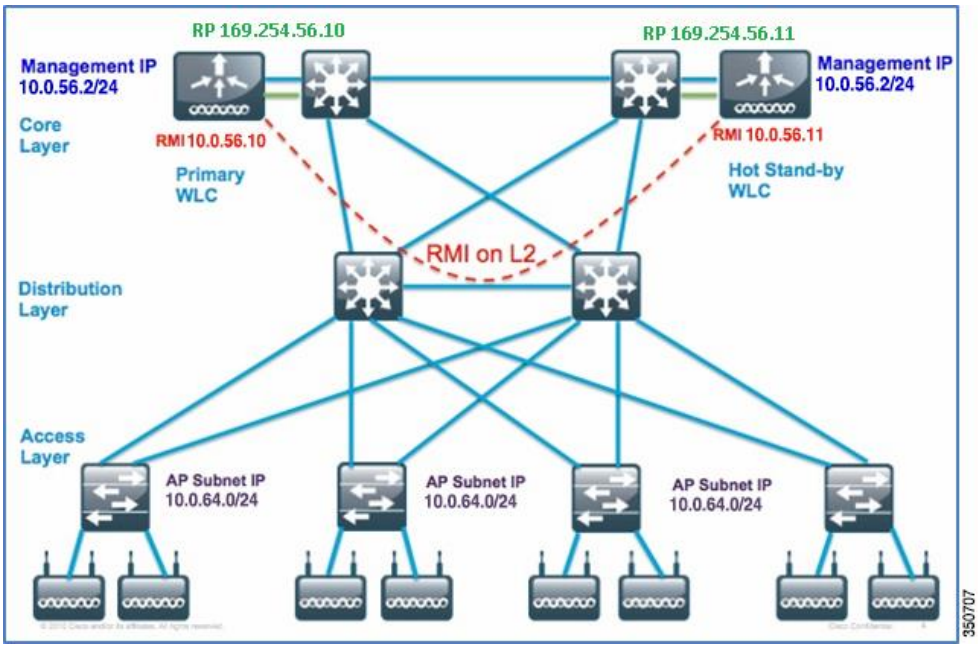
```
configure interface address management 10.0.56.2 255.255.255.0 10.0.56.1
configure interface address redundancy-management 10.0.56.10 peer-redundancy-management
10.0.56.11
configure redundancy
unit primary configure
redundancy mode sso
```

配置热备无线控制器：

```
configure interface address management 10.0.56.3 255.255.255.0 10.0.56.1
configure interface address redundancy-management 10.0.56.11 peer-redundancy-management
10.0.56.10
configure redundancy unit
secondary configure
redundancy mode sso
```

通过交换机连接冗余端口

图2 通过交换机连接冗余端口



- 跨数据中心的通过交换机连接的冗余端口连接支持这种拓扑。
- 配置同步和Keepalive消息是通过冗余端口发送的。
- RMI冗余管理接口作为管理子网的的一部分而创建，用于检查对等体和管理网关可达性。
- 默认情况下RTT延迟为80毫秒。RTT应该为keep alive计时器的80%，keep alive可配置的范围在100 - 400毫秒。
- 故障检测时间是3 * 100 = 300 + 60 = 360 + 抖动(12毫秒)= ~ 400毫秒
- 带宽：60Mbps
- MTU: 1500

配置主用无线控制器：

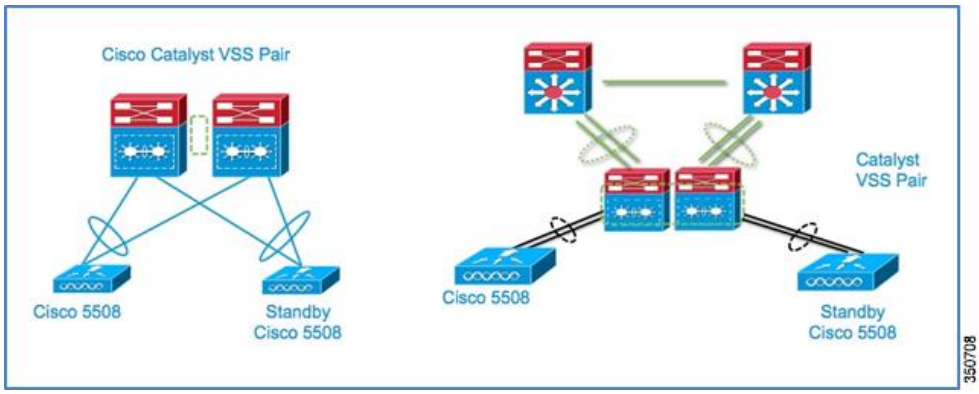
```
configure interface address management 10.0.56.2 255.255.255.0 10.0.56.1
configure interface address redundancy-management 10.0.56.10 peer-redundancy-management
10.0.56.11
configure redundancy
unit primary configure
redundancy mode sso
```

配置热备无线控制器：

```
configure interface address management 10.0.56.3 255.255.255.0 10.0.56.1
configure interface address redundancy-management 10.0.56.11 peer-redundancy-management
10.0.56.10
configure redundancy unit
secondary configure
redundancy mode sso
```

5508, 7500或8500连接到VSS配对

图3 无线控制器连接到VSS配对



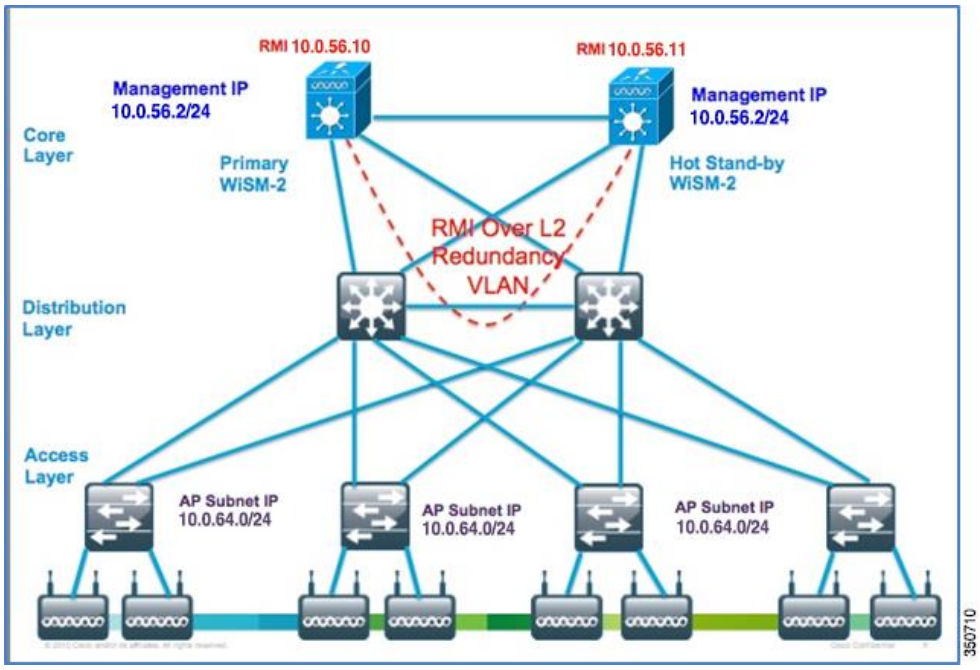
WiSM2无线控制器支持的高可用性拓扑

WiSM2在同一个机箱中

图4　单个机箱中的 WiSM2

WiSM2在不同的机箱中：2层网络的冗余VLAN

图5　WiSM2使用2层网络的冗余VLAN连接



配置Cat6k中的WiSM2无线控制器：

```
wism service-vlan 192 ( service port VLAN )
wism redundancy-vlan 169 ( redundancy port VLAN )
wism module 6 controller 1 allowed-vlan 24-38 ( data VLAN )
```

WiSM2 HA configuration remains the same.

WiSM2在不同的机箱中：VSS配对

图6　使用VSS配对的WiSM2连接

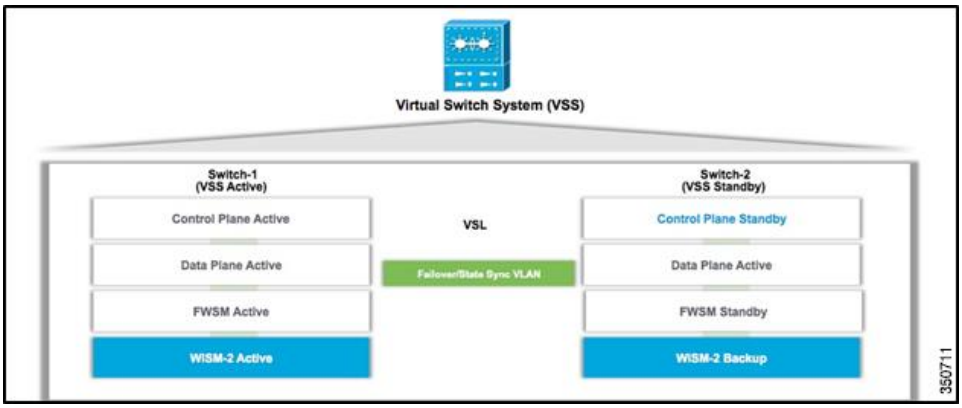


图7　使用VSL连接的VSS配对主用和备用

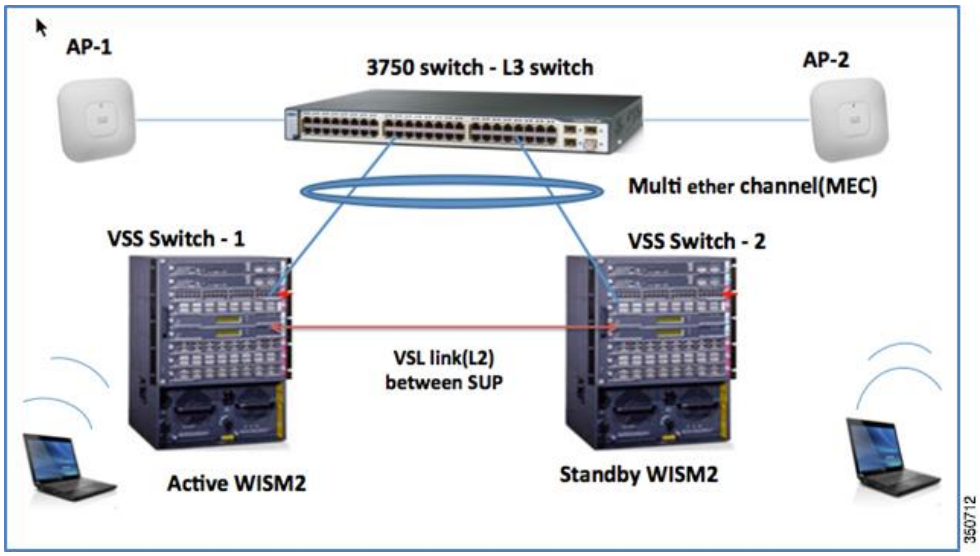
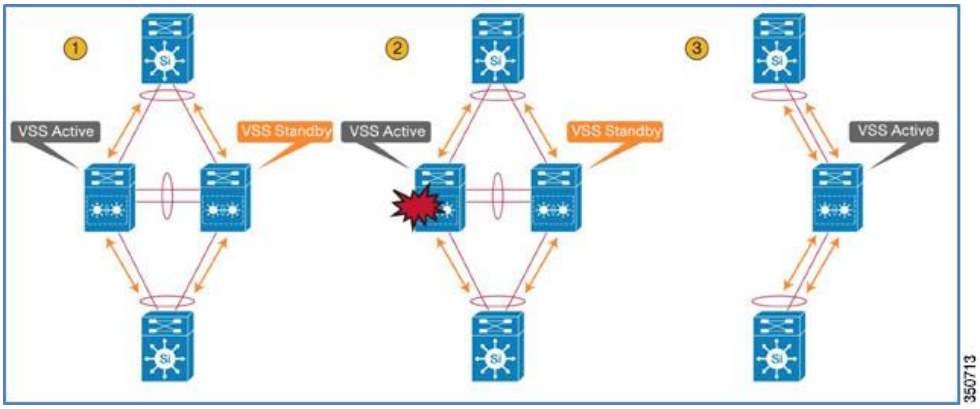


图8 使用VSS配对的WiSM2连接



VSS配置

	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

建议

- 冗余链路往返延迟时间应小于或等于80毫秒。
- 冗余链路建议MTU在1500或以上
- 冗余链路的带宽应该在60Mbps或更多。
- 如果冗余端口通过交换机连接，这样两个控制器之间是L2邻接，RP冗余端口VLAN应该被排除在接入VLAN外，在交换机上配置用于管理端口。
- 对于WiSM2通过L2网络连接两个不同的机箱,“冗余vlan”应该被排除在访问vlan外，在交换机上配置用于管理端口。
- 强烈建议为RP冗余端口连接和管理端口流量使用不同的交换机端口，以避免active - active场景。

客户端SSO

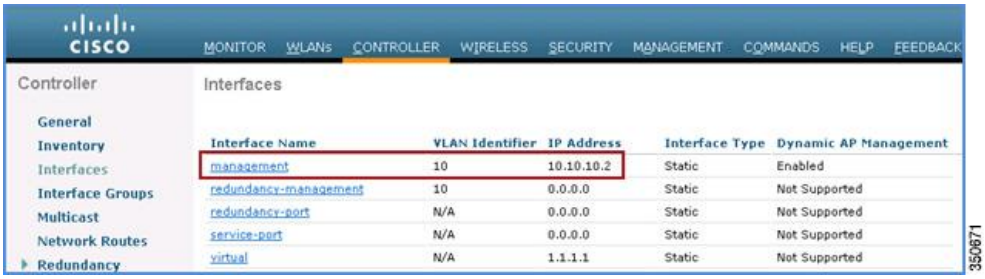
支持高可用性而不影响服务，需要支持客户端和无线接入点从主用控制器到备用控制器间的无缝切换。版本7.5在无线局域网控制器中支持客户端状态切换(客户端SSO)。客户端将支持客户端SSO，这些客户端需要已经完成了认证和DHCP阶段，并且已经开始通信。对于客户端SSO，当客户端关联或者是客户端参数改变的时候，客户的信息就会同步到备用WLC。完全经过身份验证的客户端，比如在运行状态的客户端，会同步到备用无线控制器，因此，就避免了在切换的时候客户端的重新认证，这样就使得无线接入点和客户端在故障的时候能够无缝的切换。

- 客户端SSO能在Anchor-Foreign移动性设置和Guest Anchor scenarios场景中工作。
- L3 MGIDs同步到备用无线控制器
- 根据机箱故障切换的类型的不同，故障切换时间在2 - 996毫秒之间。
- 管理网关故障切换时间为~15秒，这是12次ping管理网关的时间。
- 两个无线控制器之间的默认RTT延迟是80毫秒。RTT延迟应小于或等于keepalive计时器的80%。keepalive计时器的可配置范围在100 - 400毫秒。

配置

1. 在配置HA之前，会强制性的要求两个无线控制器的管理接口在同一子网中：

   WLC 1:

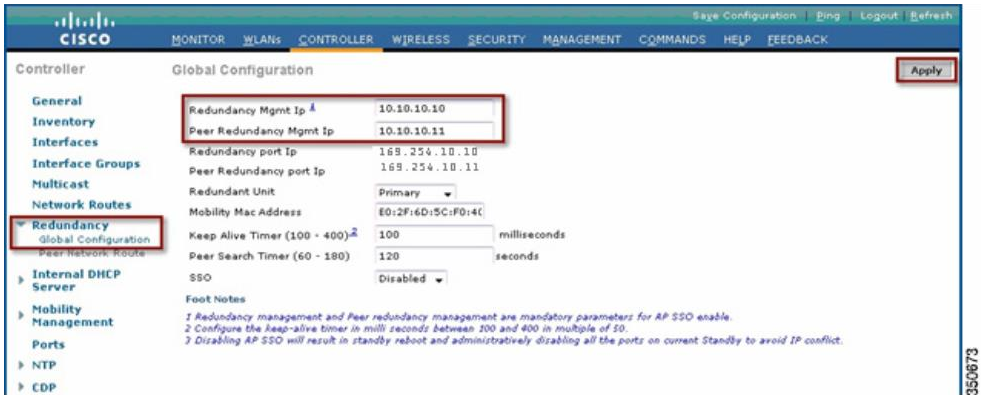


   WLC 2:

2. HA在默认情况下是不启用的。在您启用HA之前，它会强制性的配置冗余管理IP地址和对等冗余管理IP地址。这两个接口应该与管理接口在同一个子网里。

   配置冗余管理和对等冗余管理IP地址，点击 **Controller tab > Redundancy > Global Configuration**页面，在两个空白处填写IP地址，然后点击**Apply**

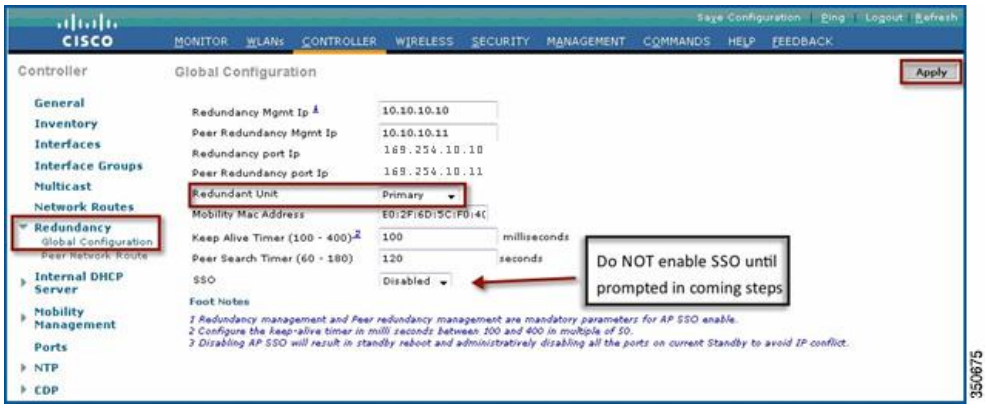
   WLC 1:



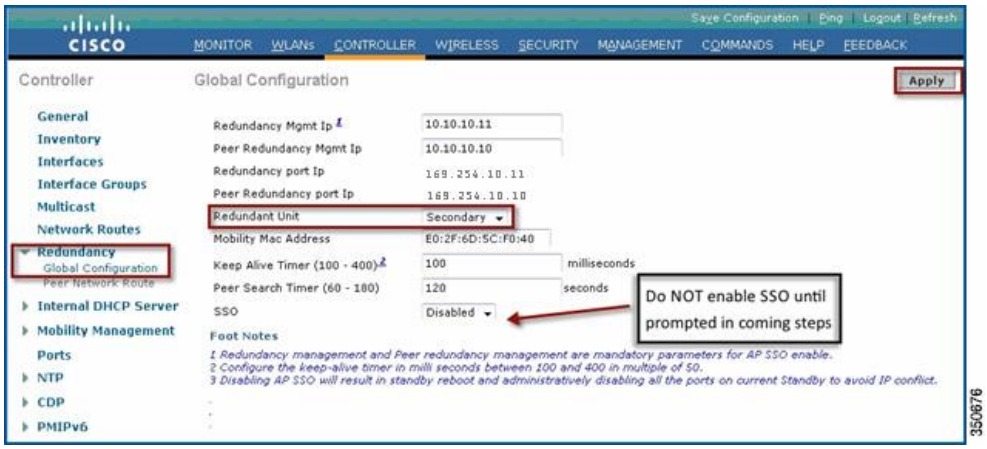
   WLC 2:

3. 在Redundant Unit的下拉列表里配置其中一个无线控制器作为主用无线控制器，另一台作为冗余无线控制器。在下边这个例子中，WLC1配置为主用控制器，WLC 2被配置为备用控制器。在配对的过程中，配置成主用的控制器会将相应数量的AP授权推送给备用无线控制器。要配置一个无线控制器配置成主用单元，第二个配置成备用单元，点击**Controller tab > Redundancy > Global Configuration**，在Redundant Unit下拉列表中选择Primary/Secondary选项，点击**Apply**。

   WLC 1:



   WLC 2:



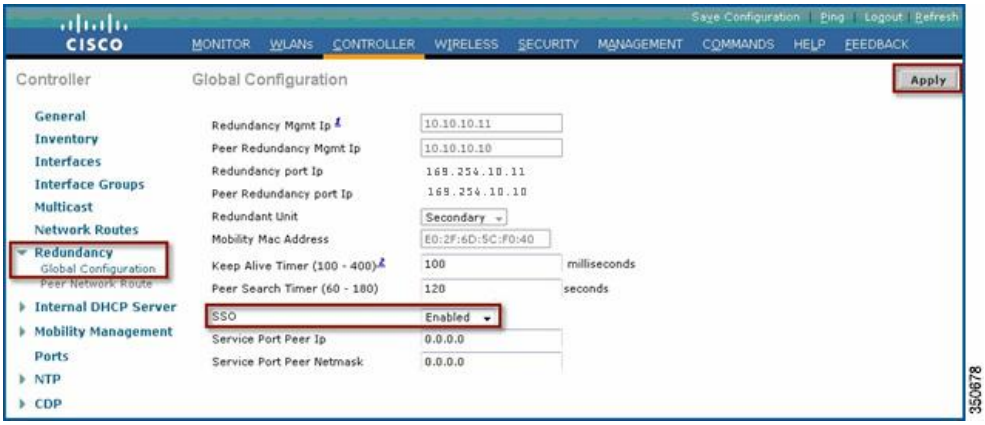
4. 在无线控制器上配置了冗余管理和对等冗余管理IP地址和冗余单元之后，一定要要确保两个无线控制器之间的物理连接是连通的，例如，无线控制器之间冗余端口使用了以太网线缆连接，上联端口连接到了基础网络交换机，并且无线控制器到无线控制器都可达。在两个无线控制器上使用Ping来确认管理接口网关IP地址的可达性，确保到管理网关的连接是完好的。

5. 要开启SSO向导，进入到**Controller >Redundancy > Global Configuration**页面下，在

SSO下拉列表选择**Enable**选项，点击**Apply**。这个步骤完成后无线控制器将会重启。

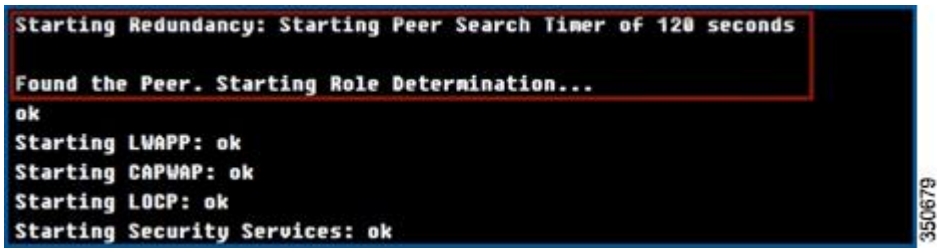
WLC 1:

WLC 2:



6. 启用SSO功能将重新启动无线控制器以便在每个配置平台上重新协商高可用性角色。当设备的角色确定后，备用无线控制器就会通过冗余端口从主用无线控制器同步配置。最初，备用无线控制器会报告XML不匹配，会从主用无线控制器上下载配置后再次重启。在高可用性角色确定后再次重新启动时，会再次验证配置，就没有XML配置不匹配的报告了，就会进行下面的流程配置使该设备成为备用无线控制器。所以，配置成主用的控制器会重启一次，备用控制器会重启两次。

   WLC 1:



   在启用SSO功能后WLC2第一次重启

```
Starting VPN Services: ok
Starting DNS Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...

Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are different, reboot required
Restarting system. Reason: rsyncmgrXferTrasport ..
Restarting system.
```

350680

WLC2从主无线控制器上下载了XML配置后，进行第二次启动:

```
Starting VPN Services: ok
Starting DNS Services: ok
Starting Licensing Services: ok
Starting Redundancy: Starting Peer Search Timer of 120 seconds

Found the Peer. Starting Role Determination...
Standby started downloading configurations from Active...

Standby comparing its own configurations with the configurations downloaded from Active...


Startup XMLs are same, no reboot required
Standby continue...
ok
Starting LWAPP: ok
Starting CAPWAP: ok
```

350681

在WLC2启动的过程当中，不能对WLC1进行任何的配置改变。

```
(POD1-WLC) >
Blocked: Configurations blocked as standby WLC is still booting up.
         You will be notified once configurations are Unblocked

Unblocked: Configurations are allowed now...
```

350682

7. 启用SSO后，无线控制器重新启动并同步XML配置，WLC 1转化为主用状态和WLC 2转化为热备份状态状态。从这时开始，WLC2上管理接口的GUI / TELNET / SSH 将无法正常工作，所有的配置和管理应该从主用无线控制器完成。如果需要的话，备用无线控制器，在里是WLC 2，只能通过服务端口或console线来管理。

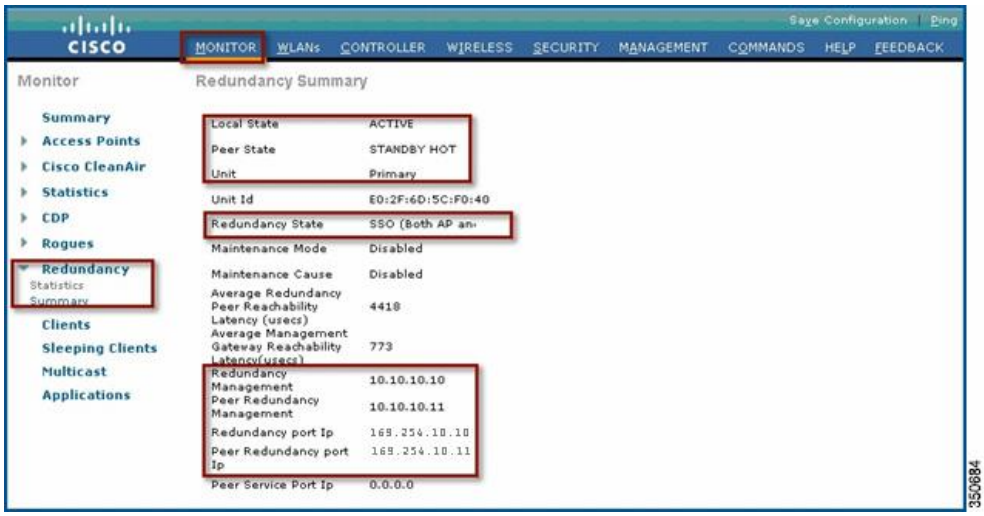
   此外，一旦对端的无线控制器转换到热备份状态，-standby关键字会自动附加到备用无线控制器的提示名称上。

```
User: admin
Password:********
(POD1-WLC-Standby) >
```

350683

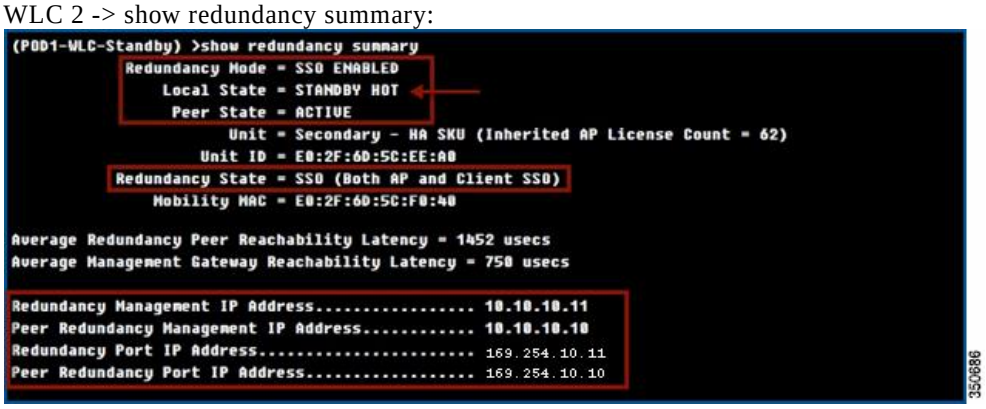
8. 检查冗余状态

   WLC 1 -> 点击 **Monitor > Redundancy > Summary:**



WLC 1 -> show redundancy summary:

WLC 2 -> show redundancy summary:



无线接入点和客户端状态同步

1. 在这个时候两个控制器在HA配置中进行了配对。所有在主用控制器的配置都会通过冗余端口同步到备用控制器。在备用控制器上通过console连接查看WLAN和接口信息总结。
2. 在高可用性配置中，无线接入点的CAPWAP状态保存在主用和备用无线控制器上（只针对于在运行状态的AP）。在下例中，WLC1是在活跃状态为网络服务，WLC2在备用状态监控者活跃的控制器。虽然WLC2在备用状态，但是也会保存无线接入点的CAPWAP状态。

   WLC 1->Console连接:

```
(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

观察在主用无线控制器上的无线接入点的运行时间和关联持续时间

WLC 2->Console连接:

```
(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

观察备用控制器上从主用控制器上同步过来的无线接入点的运行时间和管理持续时间

3. 机箱故障的情况下，例如，主用无线控制器崩溃/系统挂起/手动复位/人力切换，主用控制器会通过冗余端口和冗余管理端口发送直接命令到备用控制器来接管网络。根据网络中的无线接入点的数目，这可能要花费2-360毫秒时间。电源故障的情况下，主用无线控制器或不能发送一些直接命令进行切换，可能需要360-990毫秒，也取决于主用控制器上的无线接入点/客户端的数量和保持连接定时器的时间。默认的保持连接定时器是100毫秒。要确保默认RTT延迟时间要小于等于80毫秒。

4. 在7.5版本中的客户端SSO功能中，客户端数据库也会同步到备用无线控制器，所以运行状态客户端条目也会在备用控制器中显示。

   WLC 1-> Console/Telnet/SSH连接:

```
(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
20: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

在主用控制器上显示的客户端条目

WLC2-> Console连接:

```
(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

在备用控制器上显示的客户端条目

5. PMK缓存也会在两个无线控制器之间同步。

WLC 1:

```
(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
```

350693

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

故障切换过程

1. 在主用控制器上使用**redundancy force-switchover**命令。使用这个命令会手动的开启切换，主用控制器会重启，备用控制器会接管整个网络。在这种情况下，主用无线控制器上在运行状态的客户端不会被解除认证。需要在**redundancy force-switchover**命令前使用**save config**命令。

WLC 1-> Console连接:

```
(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-> Console连接:

```
(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 20:e7:cf:ec:e9:50
Client MAC Address............................... 20: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

在以上的抓屏中查看变化

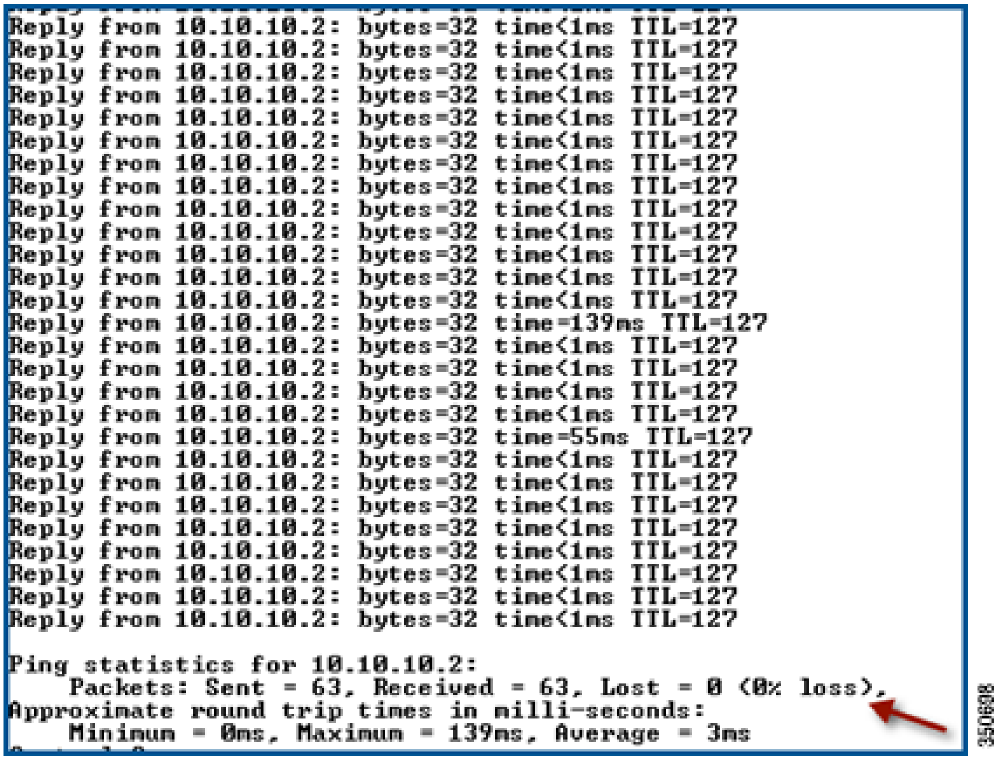
WLC 2->Console连接:

```
(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 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
```

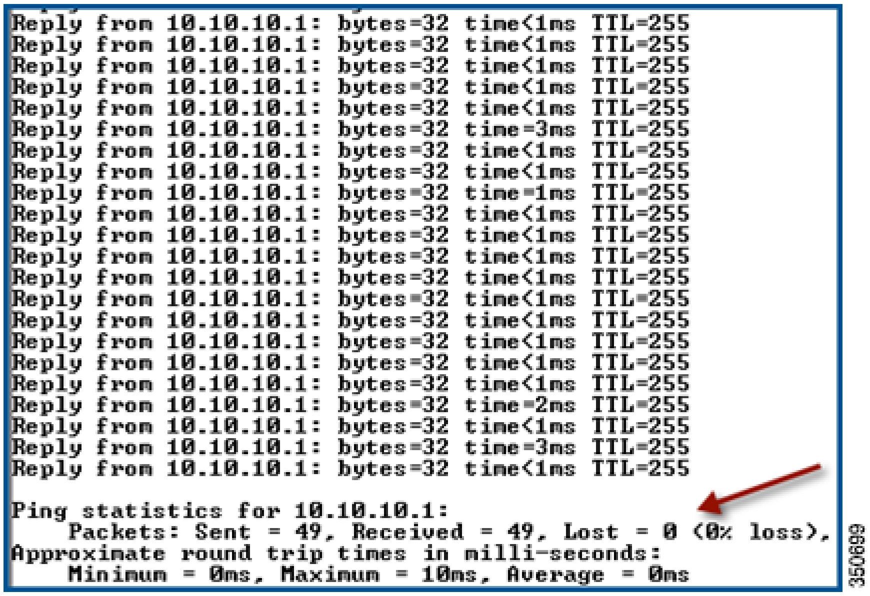
350697

查看在WLC2上AP的CAPWAP状态，最初的时候是备用控制器，在切换之后变成了主用的控制器。无线接入点运行时间以及关联持续时间都会得到保持，不会进入到查找状态。

2. 在切换发生的时候注意客户端的连接。客户端不会被结束认证。在切换过程中无线客户端Ping网关IP地址以及管理IP地址只会有极少的丢失。



```
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
```



```
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<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
```

3. 检查冗余状态

   WLC 1 -> 使用Console连接，输入命令**show redundancy summary:**

```
(POD1-WLC) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = ACTIVE
                 Peer State = STANDBY HOT
                       Unit = Secondary - HA SKU (Inherited AP License Count = 62)
                    Unit ID = E0:2F:6D:5C:EE:A0
          Redundancy State = SSO (Both AP and Client SSO)
              Mobility MAC = E0:2F:6D:5C:F0:40

Average Redundancy Peer Reachability Latency = 2660 usecs
Average Management Gateway Reachability Latency = 751 usecs

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

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
```

350700

WLC 2 ->使用 Console 连接，输入命令 **show redundancy summary**:

```
(POD1-WLC-Standby) >show redundancy summary
            Redundancy Mode = SSO ENABLED
                Local State = STANDBY HOT
                 Peer State = ACTIVE
                       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

Average Redundancy Peer Reachability Latency = 1347 usecs
Average Management Gateway Reachability Latency = 763 usecs

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

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
```

350701

WLC 2-> 点击**Monitor > Redundancy > Summary**进入到页面**:**

350702

4. 在当前的主用无线控制器上进行强制切换。

被配置成主用单元的控制器应该是活跃的，被配置成备用单元的WLC2应该是热

备状态。

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 > 在切换之后，确保本地状态是活跃状态，在WLC1上的单元是主用的。

```
(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....................... 169.254.10.11
Peer Redundancy Port IP Address.................. 169.254.10.10
Peer Service Port IP Address..................... 0.0.0.0
```

350704

观察切换历史。WLC会保存10个切换历史及其切换原因信息。

```
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

客户端SSO行为和限制

- 由服务和与一个服务相关联的服务提供商，以及域名数据库组成的Bonjour动态数据库会同步到备用控制器。
- 只有在运行状态的客户端才会在主用和备用控制器之间同步。客户端SSO功能不支持还处在关联/加入控制器过程客户端的无缝切换。还在转换阶段的客户端会在切换后解除认证，需要重新加入无线控制器。
- 如果客户端不在运行状态，就不支持Posture和NAC OOB功能
- WGB以及与WGB关联的客户端需要在切换之后重新关联
- 基于CCX的应用需要在切换之后重新开启
- 不支持与融合访问配合的移动性功能
- 客户端状态数据不会同步
- PMIPv6, NBAR, SIP静态CAC树不会同步，需要在SSO之后重新学习。

- 不支持OEAP（600系列）
- 被动客户端在SSO之后需要重新关联
- 设备和根证书不会自动的同步到备用控制器。
- 非法无线接入点和非法客户端信息不会同步到备用控制器，在热备控制器成为主用控制器之后需要重新学习。
- 睡眠状态的客户端信息不会同步到备用控制器。
- NBAR参数不会同步到备用控制器

客户端识别数据不会同步到备用控制器，因此，客户端在切换后需要进行重新分析识别。

术语表

A

AP SSO

无线接入点的状态完全转换，每个无线接入点的CAPWAP状态会在保存在主用和备用控制器，在切换到备用控制器之后会重新获得CAPWAP状态。在发生故障切换之后，无线接入点不需要经过CAPWAP发现和加入过程

Active WLC

这是在HA配对中活跃的控制器，管理着整个无线网络。无线接入点会与活跃的无线控制器建立一个单独的CAPWAP隧道

C

Client SSO

无线客户端状态完全切换，也会在主用和备用控制器上保持客户端状态信息，无线客户端在切换之后也不会结束认证。

K

Keep-Alive-Timer

在HA配置中的备用无线控制器会在冗余端口上发送keep-alive包来检查主用无线控制器的健康状态。如果没有从主用无线控制器收到三个keep-alive数据包的回复，备用控制器就会宣布主用控制器无用接手整个网络。

M

Maintenance Mode

当备用无线控制器不能与网关通信，或者是不能够通过冗余端发现对等活跃无线控制器，无线控制器口进入到维护模式。在该模式下，无线控制器不能够与其下网络通信，不能够参与到高可用性的过程中。因为在维护模式下的无线控制器不会参与到HA过程中，它需要手动地重启使其推出维护模式，才能再一次参与到HA过程中。

Mobility MAC

在HA配置中分享的唯一的MAC地址。这个MAC地址会被用来在HA配置和HA配置中的其他无线控制器或者是独立的控制器之间组成一个移动性配对。默认情况下，活跃无线控制器的mac地址会被共享成为移动性mac地址，但是移动性mac地址也可以在活跃无线控制器上使用CLI命令手动进行配置，也会在HP配置中进行配对。

P

Peer

AP SSO是机箱到机箱的冗余，例如，1:1的情况下，在HA配置中的两个无线控制器（活跃的和备用的）都是相互的对等体。

Primary Unit 在AP SSO部署，运行更多永久授权数量的无线控制器需要被配置成主用单元。主用单元是在第一次形成HA配对的时候成为活跃控制器角色的无线控制器。主用单元会通过冗余端口发送授权数量信息给它的对等体。

Peer-Search-Timer 在启动的时候，备用无线控制器会等待对等搜索计时器（默认2分钟）去发现对等体。如果无线控制器不能够在这个时间内发现对等体，它会进入到维护状态。

R

Redundancy Port 5500/7500/8500无线控制器在HA角色协商中，在主用和备用无线控制器间配置的同步和冗余信息使用的物理端口。

Redundancy Vlan Cat6500上为连接在Cat6k背板上的WiSM-2冗余端口创建的Vlan，用来在活跃和备用无线控制器之间交换包括HA角色协商以及配置和冗余信息。

Redundancy Management Interface 在HA配置中两个无线控制器上与管理接口并行的一个接口。应该与管理接口在同一个子网中。这个接口可以使备用无线控制器与其下网络交互，并且在主用和备用无线控制器之间通过其他网络交互某些冗余信息。

S

Standby WLC 在HA配对中监控着活跃控制器，当活跃控制器故障的时候掌管整个无线网络。

Secondary Unit 在AP SSO部署，运行小于或者相等永久授权数量的无线控制器需要被配置成第二单元或默认发货拥有HA SKU UDI（零个AP授权数量）的被配置成第二单元。第二单元的无线控制器会在第一次形成HA配对的时候成为备用无线控制器。第二单元会从它的对等体获得授权数量信息。例如，通过冗余端口从活跃无线控制器获得。