室内Mesh部署指南

目录

简介

轻量接入点1242/1131是用于选定室内部署的双射频Wi-Fi基础设施设备。它是基于轻量接入点协议(LWAPP)的产品。它提供2.4 GHz无线电和与802.11b/g和802.11a兼容的5.8 GHz无线电。一个无线电可用于接入点(AP)的本地（客户端）接入，第二个无线电可配置用于无线回传。LAP1242/LAP1131支持P2P、P2MP和网状架构类型。

在尝试安装之前，请务必阅读本指南。

本文档介绍室内网状网的企业无线网状网的部署。本文档将帮助无线最终用户了解室内网状网络的基础知识、在何处配置室内网状网以及如何配置室内网状网。室内网状网是使用无线控制器和轻量AP部署的思科企业无线网状网的子集。

室内网状网是部署在统一无线架构上的企业网状网架构的子集。现在，室内网状网已经需求旺盛。使用室内网状网时，其中一个无线电（通常为802.11b/g）和/或有线以太网链路用于连接客户端，而第二个无线电（通常为802.11a）用于回传客户端流量。回传可以是单跳或多跳。室内网状网为您带来以下值：

- 无需为每个AP运行以太网布线。
- 每个AP不需要以太网交换机端口。
- 网络连接，其中电线无法提供连接。
- 部署灵活性 — 不限于以太网交换机的100米。
- 易于部署点对点无线网络。

由于布线成本节省以及前面提到的原因，大盒子零售商对室内网状网络非常感兴趣。

库存专家使用它为零售商、制造厂和其他公司执行库存盘点。他们希望在客户站点快速部署临时Wi-Fi网络，以便为其手持设备实现实时连接。教育研讨会、会议、制造和招待是需要室内网状架构的场所。

阅读完本指南后，您将了解在何处使用以及如何配置室内网状网。您还将了解，NEMA外壳中的室内网状网不是室外网状网的替代品。此外，您还将了解室内网状网相对于自治AP使用的链路角色灵活性（单跳网状网）的优势。

假设：

您对思科统一无线网络、架构和产品有所了解。您了解思科室外网状网产品和一些用于网状网络的术语。

缩略词表	
LWAPP	轻量接入点协议 — AP与无线LAN控制器之间的控制和数据隧道协议。
WLAN控制器/控制器/WLC	无线LAN控制器 — 思科设备，通过将大量托管端点合并到单个统一系统中来集中并简化WLAN的网络管理

	，从而实现统一的智能信息WLAN网络系统。
RAP	根接入点/屋顶接入点 — 思科无线设备充当控制器与其他无线AP之间的桥。连接到控制器的AP。
映射	网状AP — 在802.11a无线电上通过空连接到RAP或MAP的思科无线设备，还在802.11b/g无线电上为客户端提供服务。
父	AP(RAP/MAP)，通过802.11a无线电提供对其他AP的空中访问。
邻居	网状网络中的所有AP都是邻居，且具有邻居。RAP与控制器连接时没有邻居。
子	远离控制器的AP始终是子AP。子网在网状网络中将有一个父网和多个邻居。如果父节点死亡，则具有最佳缓动值的下一个邻居将选择父节点。
SNR	信噪比
BGN	网桥组名称
EAP	可扩展认证协议
PSK	预共享密钥
AWPP	自适应无线路径协议

概述

思科室内网状网络接入点是用于选定室内部署的双射频Wi-Fi基础设施设备。它是基于轻量接入点协议(LWAPP)的产品。它提供2.4 GHz无线电和5.8 GHz无线电，与802.11b/g、802.11a标准兼容。一个无线电(802.11b/g)可用于AP的本地（客户端）访问，第二无线电(802.11a)可配置用于无线回传。它提供室内网状网架构，其中不同节点（无线电）通过回传彼此通信，并提供本地客户端访问。此AP也可用于点对点和点对多点桥接架构。无线室内网状网络解决方案非常适合于大型室内覆盖，因为您能够以最低的基础设施实现高数据速率和良好的可靠性。以下是本产品首次发布时引入的基本突出功能：

- 用于室内环境，跳数为3。最多4个。
- 最终用户客户端的中继节点和主机。802.11a无线电用作回传接口，802.11b/g无线电用于为客户端提供服务。
- 室内网状AP安全 — 支持EAP和PSK。
- 网状环境中的LWAPP MAP与控制器通信的方式与连接以太网的AP相同。
- 点对点无线桥接。
- 点对多点无线桥接。
- 最佳父项选择。SNR、EASE和BGN
- BGN增强功能。NULL和默认模式。

- 本地访问。
- 父黑名单。排除列表。
- 使用AWPP进行自我修复。
- 以太网桥接。
- 4.0版本对语音的基本支持。
- 动态频率选择.
- 防绞合 — 默认BGN和DHCP故障转移。

注意：将不支持以下功能：

- 4.9 GHz公共安全信道
- 围绕干扰进行路由
- 背景扫描
- 通用访问
- 工作组网桥支持

室内网状网软件

室内网状网软件是一种特殊版本，因为它专注于室内AP，尤其是室内网状网。在此版本中，室内AP在本地模式和桥接模式下都工作。4.1.171.0版本中提供的一些功能未在此版本中实施。对命令行界面(CLI)、图形用户界面（GUI - Web浏览器）和状态机本身进行了改进。这些改进的目的是从您的角度获得有关此新产品及其功能可行性的宝贵信息。

室内网状网特定增强功能：

- **室内环境** — 室内网状网是使用LAP1242和LAP1131实现的。这些网状网是在没有以太网电缆的室内环境中实现的。实施过程简单且快速，可为建筑内的偏远地区（例如，零售配送中心、研讨会/会议教育、制造业、酒店业）提供无线覆盖。
- **网桥组名称(BGN)增强功能** — 为了让网络管理员将室内网状AP网络组织到用户指定的扇区中，思科提供了一种称为网桥组名称(BGN)的机制。BGN（实际上是扇区名称）使AP连接到具有相同BGN的其他AP。如果AP找不到与其BGN匹配的适当扇区，则AP在默认模式下运行，并选择响应默认BGN的最佳父级。此功能在与搁浅的AP条件（如果某人配置了错误的BGN）进行斗争时，已收到现场的许多赞赏。 在4.1.171.0软件版本中，当使用默认BGN时，AP不作为室内网状节点运行，也没有任何客户端访问。它处于维护模式，可通过控制器访问，如果管理员不修复BGN，AP将在30分钟后重新启动。
- **安全增强**功能 — 默认情况下，室内网状代码的安全配置为EAP（可扩展身份验证协议）。RFC3748中对此进行了定义。虽然EAP协议不限于无线LAN，而且可用于有线LAN身份验证，但最常用于无线LAN。当802.1X启用的NAS（网络接入服务器）设备（如802.11 a/b/g无线接入点）调用EAP时，现代EAP方法可以提供安全身份验证机制并在客户端和NAS之间协商安全PMK（对向主密钥）。然后，PMK可用于使用TKIP或CCMP（基于AES）加密的无线加密会话。在4.1.171.0软件版本之前，室外网状AP使用PMK/BMK加入控制器。这是一个三个周期的过程。现在，缩短了周期以加快收敛。室内网状网络安全的总体目标是：零接触配置，用于调配安全性。数据帧的隐私和身份验证。网络和节点之间的相互身份验证。能够使用标准EAP方法对室内网状AP节点进行身份验证。分离LWAPP和室内网状网安全。发现、路由和同步机制从当前架构中得到增强，以适应支持新安全协议所需的元素。室内网状AP通过扫描和侦听来自其他网状AP的无故邻居更新来发现其他网状AP。连接到网络的任何RAP或室内MAP在其NEIGH_UPD帧（与802.11信标帧非常相似）中通告核心安全参数。此阶段结束后，室内网状AP和根AP之间将建立逻辑链路。
- **WCS增强功能**已添加室内网状警报。可以生成显示跳数、最差SNR等的室内网状网报告。链路测试（父到子、子到父）可以在显示非常智能信息的节点之间运行。显示的AP信息比之前的

AP信息多得多。您还可以选择查看潜在邻居。健康监控得到改进，访问更方便。

支持的硬件与软件

室内网状网有最低的硬件和软件要求：

- Cisco LWAPP AP AIR-LAP1242AG-A-K9和AIR-LAP1131AG-A-K9支持室内网状配置。
- 思科网状网版本2软件支持企业网状网（室内和室外产品）。 这只能安装在思科控制器、思科440x/210x和WISM上。
- 思科企业网状网版本2软件可从Cisco.com下载。

室内与室外

以下是室内和室外网状网的一些显着区别：

	室内网状	室外网状
环境	仅室内，硬件室内额定	仅室外，坚固型硬件
Hardware	使用LAP1242和LAP1131AG的室内AP	使用LAP15xx和LAP152x的室外AP
功率电平	2.4 Ghz:20dbm 5.8 Ghz:17dbm	2.4 Ghz:28dbm 5.8 Ghz:28dbm
单元格大小	约150英尺	约1000英尺
实施高度	离地面12英尺	离地面30-40英尺

配置

在开始实施之前，请务必仔细阅读本指南，尤其是在您收到新硬件时。

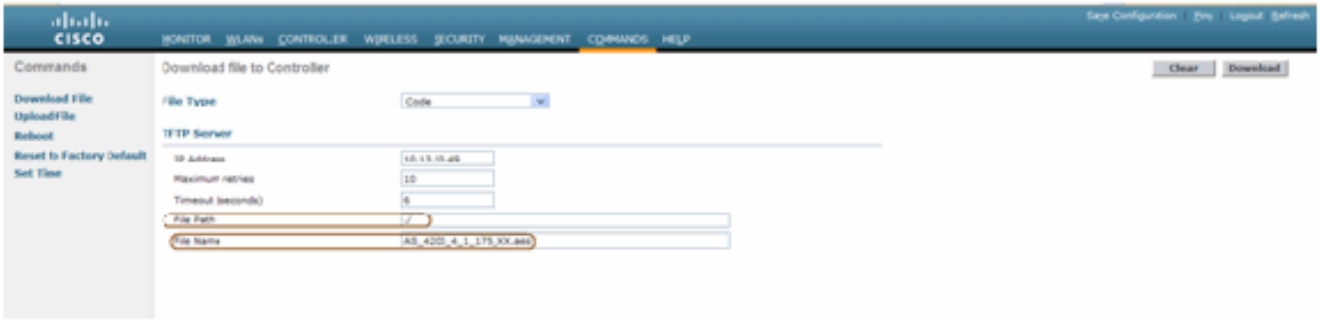
控制器L3模式

室内网状AP可部署为L3网络。

将控制器升级到最新代码

请完成以下步骤：

1. 要升级室内网状网络中的网状网版本2，您的网络必须运行在4.1.185.0或网状网版本1上（可在Cisco.com上使用）。
2. 将控制器的最新代码下载到TFTP服务器。在控制器GUI界面中，单击“命令”>“下载**文件”**。
3. 选择File type（文件类型）作为**代码**，并提供TFTP服务器的IP地址。定义文件的路径和名称。



注意：使用支持32 MB以上文件大小传输的TFTP服务器。例如，**tftpd32.**在File path put"。**/"下，如**图所示。

4. 安装完新固件后，在CLI中使用**show sysinfo**命令验证新固件是否已安装。

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

注意：从官方角度讲，思科不支持控制器降级。

Mac 地址

必须使用MAC过滤。此功能使思科室内网状网解决方案成为真正的“零接触”。 与以前版本不同，网状网屏幕将不再具有MAC过滤选项。

注意：MAC过滤默认启用。

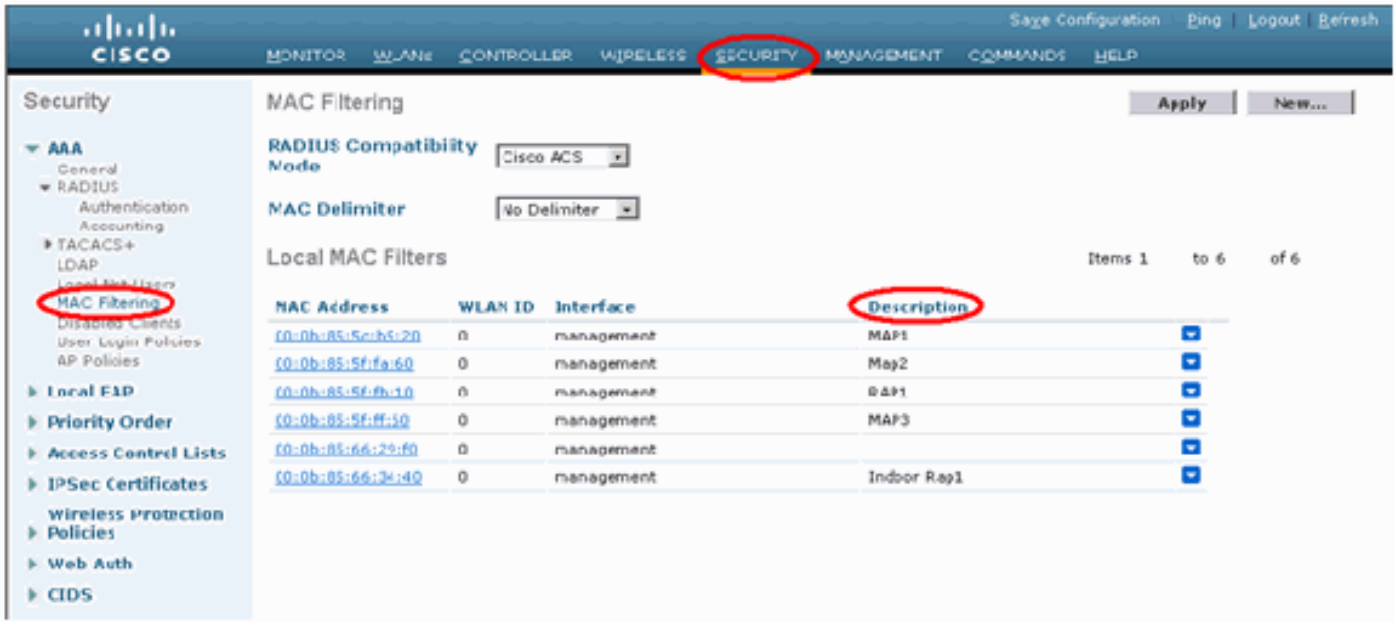
将MAC地址记录到无线电

在文本文件中，记录您在网络中部署的所有室内网状AP无线电的MAC地址。MAC地址可在AP背面找到。这有助于您进行未来测试，因为大多数CLI命令都要求使用命令输入AP的MAC地址或名称。您还可以将AP的名称更改为更容易记住的名称，例如“building number-pod number-AP type:最后四个MAC地址十六进制字符。”

在控制器中输入MAC地址和无线电的名称

思科控制器维护室内AP授权MAC地址列表。控制器仅响应来自室内无线电的发现请求，这些请求显示在授权列表上。在控制器上输入您倾向于在网络中使用的所有无线电的MAC地址。

在控制器GUI界面上，转到**Security**，然后单击屏幕左侧的**MAC过**滤。单击**New**以输入MAC地址，如下所示：



此外，在“说明”(Description)下输入无线电的名称（如位置、AP号等），以方便使用。 说明还可用于无线电设备的安装位置，以便随时参考。

启用MAC过滤

默认情况下，MAC过滤处于启用状态。

也可以在同一页面选择安全模式作为EAP或PSK。

从交换机的GUI界面，使用以下路径：

GUI接口路径：**无线>室内网状**

安全模式只能通过以下命令在CLI上检查：

```
(Cisco Controller) > show network
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

L3室内网状部署

对于L3室内网状网络，如果您不打算使用DHCP服务器（内部或外部），请配置无线电的IP地址。

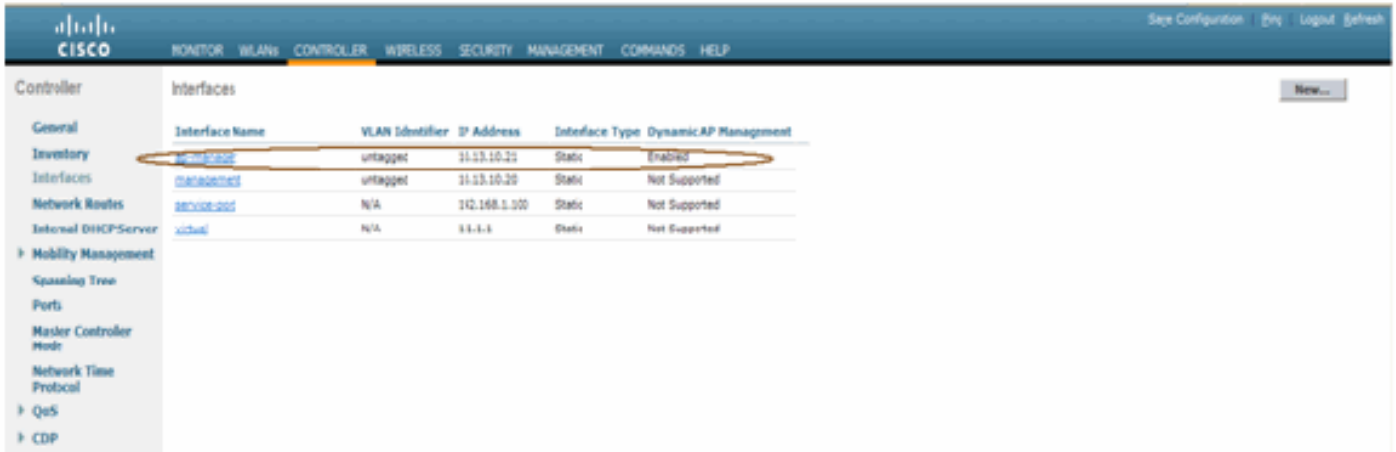
对于L3室内网状网络，如果要使用DHCP服务器，请在L3模式下配置控制器。保存配置并重新启动控制器。确保在DHCP服务器上配置选项43。控制器重新启动后，新连接的AP将从DHCP服务器接收其IP地址。

在控制器上定义接口

AP管理器

对于L3部署，必须定义**AP管理器**。AP管理器用作从控制器到AP通信的源IP地址。

路径：Controller > Interfaces > ap-manager > edit。



应为**AP管理器**接口分配一个与管理接口位于同一子网和VLAN中的IP地址。

无线电角色

此解决方案可能有两个主要无线电角色：

- 根接入点(RAP) — 要连接到控制器（通过交换机）的无线电将充当RAP的角色。RAP与控制器之间有一个支持LWAPP的有线连接。RAP是任何桥接或室内网状网络的父节点。控制器可以具有一个或多个RAP，每个RAP承担相同或不同的无线网络。同一室内网状网络可以有多个RAP以实现冗余。
- 室内网状无线接入点(MAP) — 没有与控制器有线连接的无线电充当室内网状无线接入点。此AP以前称为Pole top AP。MAP具有无线连接（通过回传接口），可能连接到其他MAP，最后连接到RAP，从而连接到控制器。MAP也可以有线以太网连接到LAN，并作为该LAN的网桥终端（使用P2P或P2MP连接）。 如果正确配置为以太网网桥，则可能同时发生这种情况。MAP为带内未用于回传接口的客户端提供服务。

AP的默认模式是MAP。

注意：无线电角色可通过GUI或CLI设置。角色更改后，AP将重新启动。

注意：如果AP物理连接到交换机，或者您可以将交换机上的AP视为RAP或MAP，则可以使用控制器CLI在AP上预配置无线电角色。

```
(Cisco Controller) >config ap role ?

rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

网桥组名称

网桥组名称(BGN)控制AP的关联。BGN可以对无线电进行逻辑分组，以避免同一信道上的两个网络相互通信。如果您的网络在同一扇区（区域）中有多个RAP，则此设置也很有用。 BGN是最多包含十个字符的字符串。

工厂集网桥组名称在制造阶段分配（NULL值）。 你看不到它。因此，即使没有定义的BGN，无线电仍然可以加入网络。如果您的网络中在同一扇区中有两个RAP（为了获得更多容量），建议您使用相同的BGN，但在不同的信道上配置两个RAP。

注意：可以从控制器CLI和GUI设置网桥组名称。

```
(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.
```

配置BGN后，AP将重置。

注意：BGN应在实时网络上配置得非常小心。您应始终从最远的节点（最后一个节点）开始，然后向RAP移动。原因是，如果您开始在多跳中间的某个位置配置BGN，则超出此点的节点将被丢弃，因为这些节点将具有不同的BGN（旧BGN）。

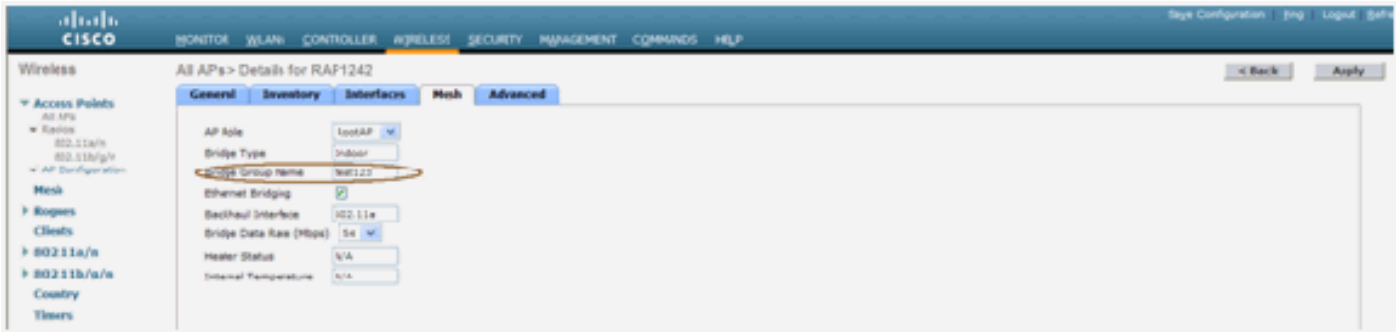
您可以通过发出以下CLI命令来验证BGN:

(Cisco Controller) **> show ap config general**

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... RAP1242
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:18:74:fa:7d:1f
IP Address Configuration......................... DHCP
IP Address....................................... 10.13.13.11
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch........................... 
Tertiary Cisco Switch............................ 
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
AP Role ......................................... RootAP
Ethernet Bridging ............................... Enabled
Bridge GroupName ................................ test123
Public Safety ..................................  Disabled
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.1.175.19
Boot  Version ................................... 12.3.7.1
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Disabled
PoE Power Injector MAC Addr...................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation.......... Disabled
Console Login Name............................... 
Console Login State.............................. Unknown
AP Up Time....................................... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time................................. 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time............................... Sun Aug 19 11:59:07 2007

Join Taken Time.................................. 0 days, 00 h 00 m 24 s
Ethernet Port Duplex............................. Unknown
Ethernet Port Speed.............................. Unknown
```

此外，您还可以使用控制器GUI配置或验证BGN:

路径：**无线>所有AP >详细信息。**



您可以看到，AP的环境信息也随此新版本一起显示。

安全配置

默认室内网状安全模式为EAP。这意味着除非您在控制器上配置这些参数，否则您的MAP将不会加入：

室内网状EAP配置CLI

```
(Cisco Controller) >config mesh local-auth enable

 enable Local Auth

(Cisco Controller) >config advanced eap ?

identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index       Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

如果需要保持PSK模式，请使用以下命令返回PSK模式：

```
(Cisco Controller) >config mesh security psk ?

(Cisco Controller) >config mesh security psk

 All Mesh AP will be rebooted
 Are you sure you want to start? (y/N)n
```

室内网状EAP show命令

在EAP模式下，您可以检查以下**show**命令以验证MAP身份验证：

```
(Cisco Controller) >show network

RF Network Name.............................. jaggi123
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Enable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Disable
Bridge Security Mode......................... EAP  otherwise PSK
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
AP Fallback ................................. Enable
Web Auth Redirect Ports ..................... 80
--More-- or (q)uit
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

(Cisco Controller) >**show wlan 0**

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500L1EAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ......................................... Disabled
   IP Security Passthru.......................... Disabled
   Web Based Authentication...................... Disabled
   Web-Passthrough............................... Disabled
   Conditional Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
--More-- or (q)uit
   H-REAP Local Switching........................ Disabled
   Infrastructure MFP protection................. Enabled (Global Infrastructure MFP Disabled)
   Client MFP.................................... Optional
   Tkip MIC Countermeasure Hold-down Timer....... 60

 Mobility Anchor List
 WLAN ID       IP Address       Status
```

(Cisco Controller) >**show local-auth config**

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries........... 20
EAP Key-Index for Dynamic WEP.............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 1
EAP-Request Max Retries.................... 2
```

```
(Cisco Controller) >show advanced eap
```

室内网状EAP调试命令

要调试任何EAP模式问题，请在控制器中使用以下命令：

```
(Cisco Controller) >debug dot1x all enable

(Cisco Controller) >debug aaa all enable
```

安装

前提条件

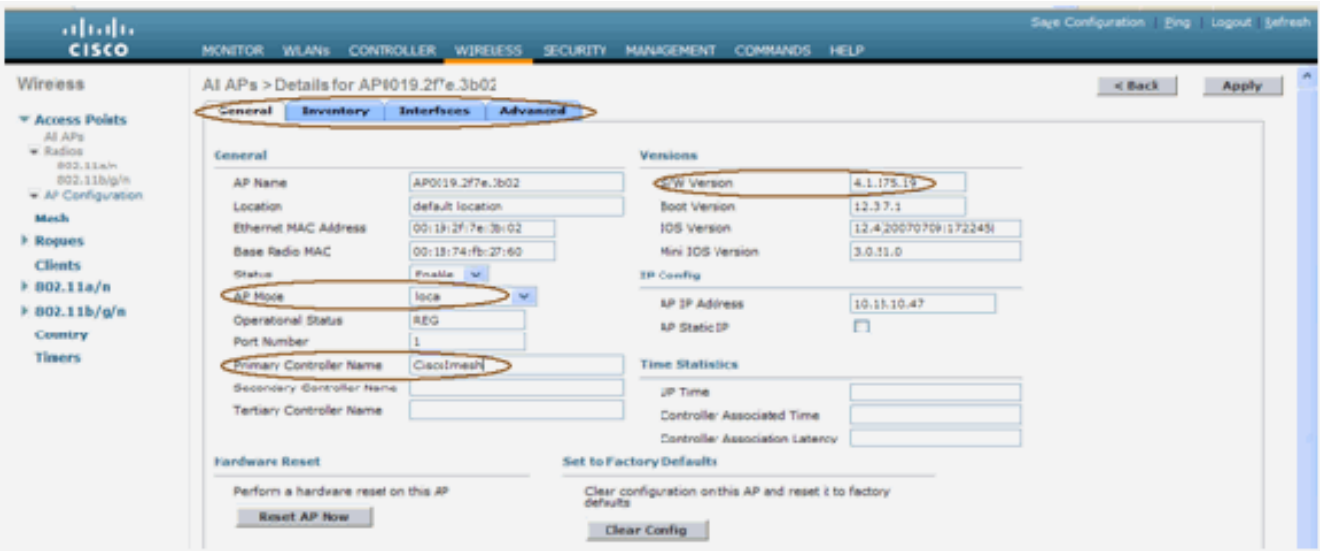
控制器必须运行推荐的代码版本。单击Monitor以验证软件版本。同样的情况可以通过CLI进行验证。

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoMesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

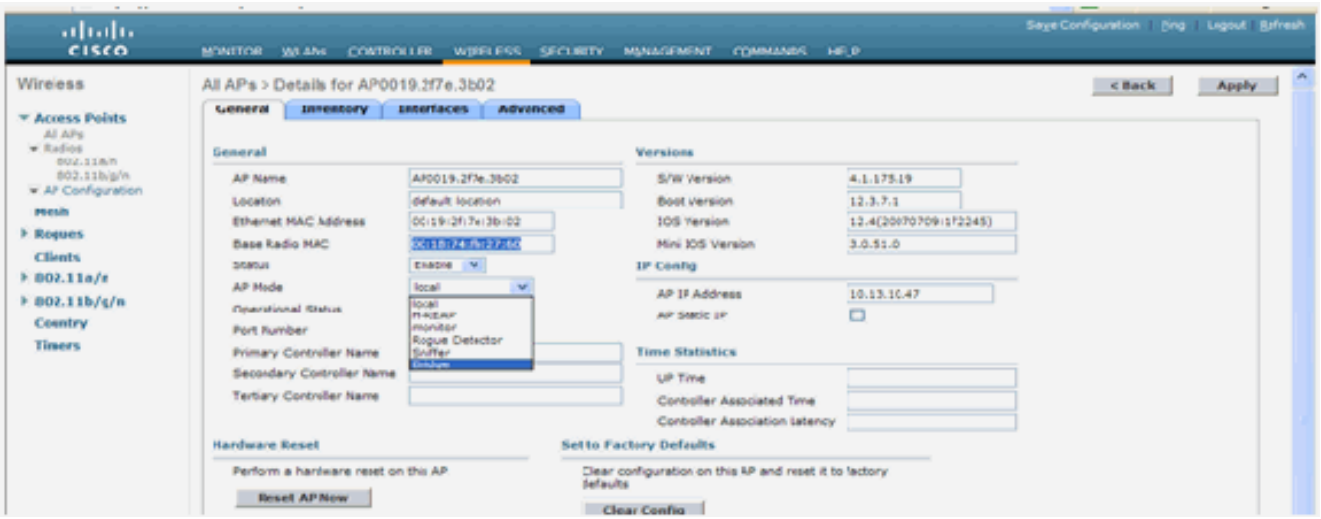
DHCP服务器、ACS服务器和WCS服务器等系统应可访问。

安装

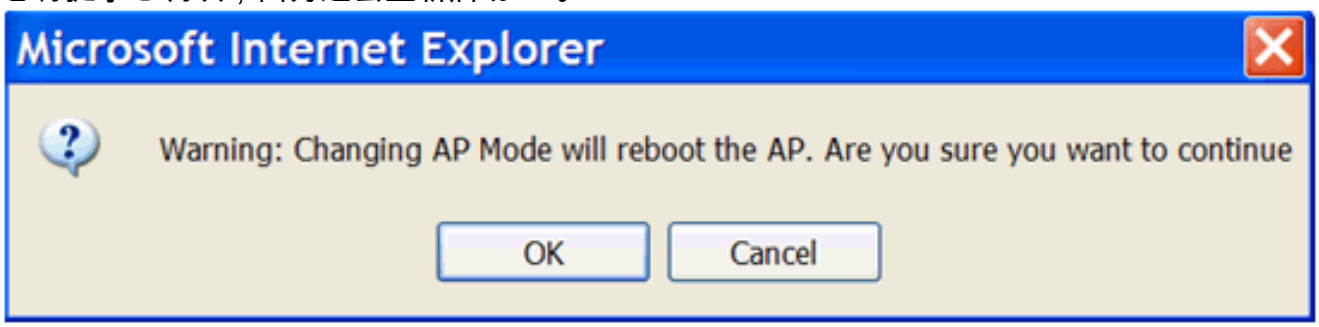
1. 将所有LAP(1131AG/1242AG)连接到与管理IP地址位于同一子网的第3层网络。所有AP将作为AP以本地模式加入控制器。在此模式下，使用主控制器名称、辅助控制器名称和第三控制器名称对AP进行首选。



2. 捕获AP的基本无线电MAC地址(例如00:18:74:fb:27:60)。
3. 添加AP的MAC地址，使AP在网桥模式下加入。
4. 单击**Security > MAC-filtering > New**。
5. 添加复制的MAC地址，并在MAC过滤器列表和AP列表中为AP命名。
6. 从AP**模式**列表**中选择**网桥。



7. 它将提示您确认，因为这会重新启动AP。



8. AP将重新启动并在网桥模式下加入控制器。新的AP窗口将有一个额外的选项卡：网状。单击**MESH**选项卡以验证角色、网桥类型、网桥组名称、以太网桥接、回程接口、网桥数据速率等

。

9. 在此窗口中，访问AP角色列表并选择相关角色。在这种情况下，默认角色为MAP。默认情况下，网桥组名称为空。回程接口为802.11a。网桥数据速率（即回传数据速率）为24Mbps。
10. 将要用作RAP的AP连接到控制器。在所需位置部署无线电(MAP)。打开无线电。您应该能够看到控制器上的所有无线电。

```
(Cisco Controller) >show ap summ

Number of APs.................................... 3

AP Name             Slots  AP Model              Ethernet MAC       Location          Port  Country
-----------------   -----  -------------------   -----------------  ----------------  ----  -------
RAP1242               2    AIR-LAP1242AG-A-K9    00:18:74:fa:7d:1f  default location  1     US
LAP1242-1             2    AIR-LAP1242AG-A-K9    00:1b:2b:a7:ad:bf  default location  1     US
LAP1242-2             2    AIR-LAP1242AG-A-K9    00:14:1b:59:07:af  default location  1     US
```

11. 尝试在节点之间设置视线条件。如果视距条件不存在，请创建菲涅耳区域间隙以获得近距位置条件。
12. 如果有多个控制器连接到同一室内网状网络，则必须在每个节点上指定主控制器的名称。否则，首先看到的控制器将作为主控制器。

电源和通道配置

回传信道可以在RAP上配置。MAP将调整到RAP信道。本地访问可以单独为MAP配置。

在交换机GUI中，遵循以下路径：**无线> 802.11a无线电> configure**。

注意：回传上的默认Tx功率级别是最高功率级别（1级），默认情况下，无线电资源管理(RRM)为OFF。

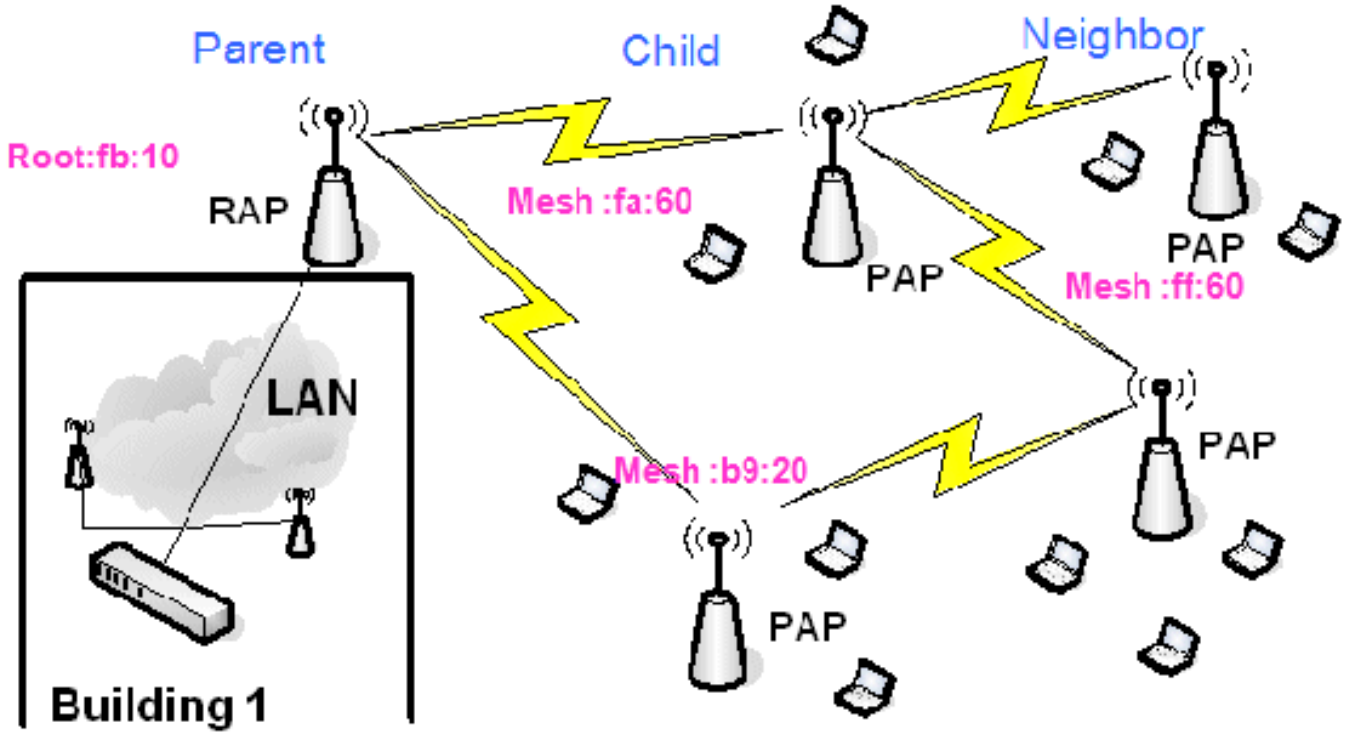
如果您正在配置RAP，我们建议您在每个RAP上使用备用相邻信道。这将减少同信道干扰。

射频检查

在室内网状网络中，必须检验节点之间的父子关系。**跳数**是两个无线电之间的无线链路。在网络中传输时，父子关系会发生变化。这取决于您在室内网状网络中的位置。

在无线连接（跳）中靠近控制器的无线电是跳**路**另一侧无线电的父无线电。在多跳系统中，有一种树型结构，其中连接到控制器的节点是RAP(父**级**)。 第一跳另一端的直接节点是子节点，**而第二跳的后续节点是该特定父**节点的邻居。

图 1：两跳网络



在图1中，为方便起见，提到了AP名称。在下一屏幕截图中，**正在研究RAP(fb:**10)。此节点可以（在实际部署中）将室内网状AP（**fa:60和b9:20）视**为子节点,**MAP ff:60为邻居**。

在交换机GUI界面中，遵循路径：**Wireless > All APs > Rap1 > Neighbor Info**。

确保为室内网状网络正确建立和维护父子关系。

检验互连

show Mesh是用于验证网络中互联的信息性命令。

您必须使用控制器CLI在每个节点(AP)上提供这些命令，并将结果上传到上传站点的Word或文本文件。

```
(Cisco Controller) >show mesh ?

env             Show mesh environment.
neigh           Show AP neigh list.
path            Show AP path.
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

在室内网状网络中，选择多跳链路并从RAP开始发出这些命令。将命令的结果上传到上传站点。

在下一节中，为图1所示的两跳室内网状网络发出了所有这些命令。

显示室内网状网路径

此命令将显示MAC地址、节点的无线电角色、上行链路/下行链路(SNRUp、SNRDown)的dB中的信噪比和特定路径的dB中的链路SNR。

```
(Cisco Controller) >show mesh path RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
RAP1242           is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-1           56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242             56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242           is a Root AP.
```

显示室内网状网邻居摘要

此命令将显示dB中的MAC地址、父子关系和上行链路/下行链路SNR。

```
(Cisco Controller) >show mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      0      0        0        0x860    BEACON
LAP1242-1           56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242             56      43     46       31       0x86b    UPDATED NEIGH PARENT BEACON
```

此时，您应该能够查看网络节点之间的关系，并通过查看每条链路的SNR值来检验RF连接。

AP控制台访问安全

此功能增强了AP控制台访问的安全性。使用此功能需要AP的控制台电缆。

支持以下功能：

- 将用户ID/密码组合推送到指定AP的CLI:

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- 将用户名/密码组合推送到注册到控制器的所有AP的CLI命令：

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

通过这些命令，从控制器推送的用户ID/密码组合在AP的重新加载过程中是持久的。如果从控制器清除AP，则不存在安全访问模式。AP生成登录成功的SNMP陷阱。AP还将连续三次在控制台登录失败时生成SNMP陷阱。

以太网桥接

出于安全原因，MAP上的以太网端口默认为禁用状态。只能通过在RAP和相应MAP上配置以太网桥接来启用它。

因此，必须为以下两种情况启用以太网桥接：

- 当您要将室内网状节点用作网桥时。
- 当您想使用MAP的以太网端口连接MAP上的任何以太网设备（如PC/笔记本电脑、视频摄像头等）时。

路径：**无线**>单击任意AP >**网状**。

CLI命令可用于配置执行桥接的节点之间的距离。尝试在每一跳连接以太网设备（如视频摄像头）并查看性能。

网桥组名称增强

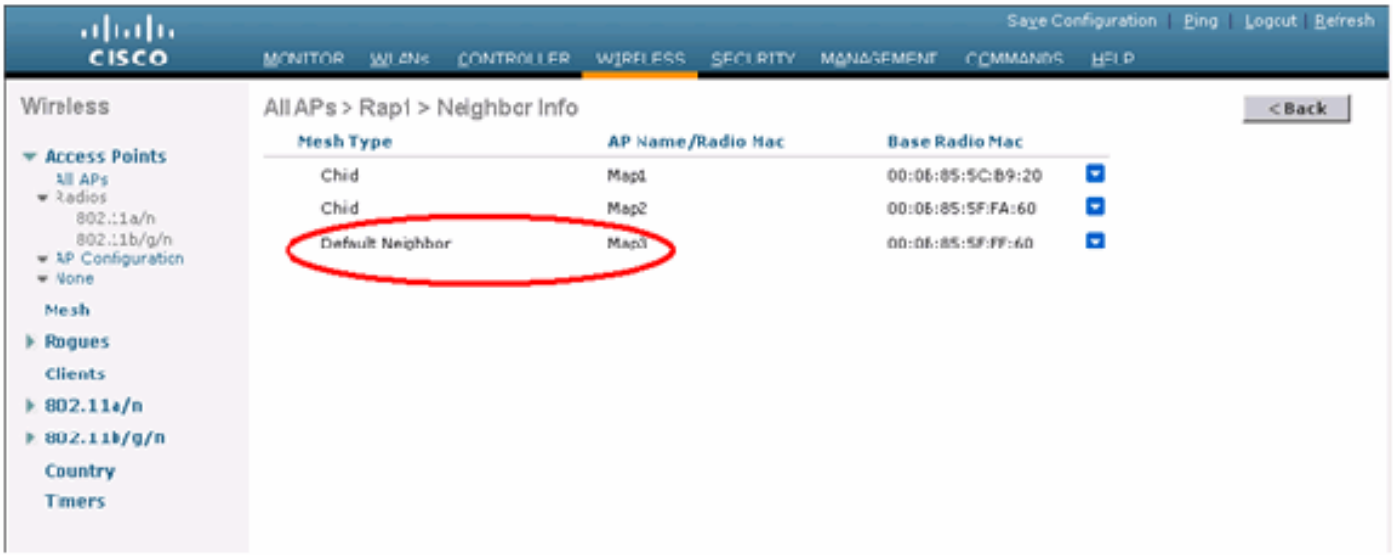
AP可能被错误地调配了“桥组名”，而它并非为此设计的。根据网络设计，此AP可能无法到达并找到其正确的扇区/树。如果它无法到达兼容的扇区，它可能会陷入困境。

为了恢复这样的搁浅AP，3.2.xx.x代码引入了“default”桥组名称的概念。基本思想是，如果AP无法使用其已配置的桥组名连接到任何其他AP，则尝试以“default”（单词）作为桥组名连接。运行3.2.xx.x及更高版本软件的所有节点都接受具有此桥组名称的其他节点。

此功能还有助于将新节点或配置错误的节点添加到运行的网络。

如果您有正在运行的网络，请使用带有不同BGN的预配置AP并使其加入网络。在控制器中添加此AP的MAC地址后，您将在控制器中看到使用“默认”BGN的此AP。

```
(CiscoController) >show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
 linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



使用默认BGN的AP可以充当正常室内网状AP，关联客户端并形成室内网状父子关系。

当使用默认BGN的此AP找到另一个具有正确BGN的父AP时，它将切换到该AP。

日志 — 消息、系统、AP和陷阱

消息日志

启用消息日志的报告级别。从控制器CLI发出以下命令：

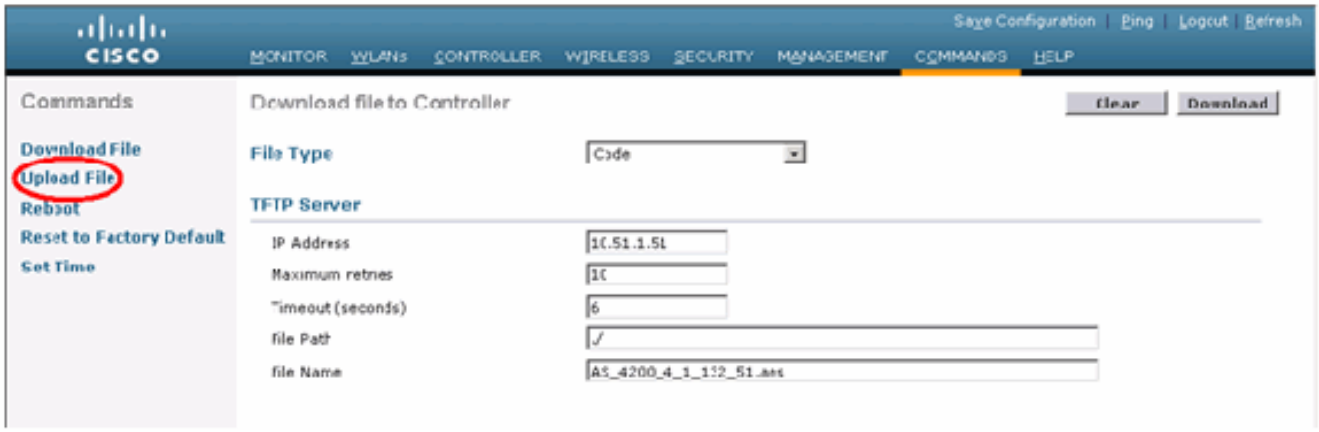
```
(Cisco Controller) >config msglog level ?

critical        Critical hardware or software Failure.
error           Non-Critical software error.
security        Authentication or security related error.
warning         Unexpected software events.
verbose         Significant system events.

(Cisco Controller) >config msglog level verbose
```

要查看消息日志，请从控制器CLI发出以下命令：

```
(Cisco Controller) >show msglog

Message Log Severity Level ..................... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul  8 06:12:02 2005  [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul  8 05:40:15 2005  [ERROR] spam_tmr.c 501: Did not receive hearbeat reply
 from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  8 05:38:40 2005  Previous message occurred 5 times
Fri Jul  8 05:33:54 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

要上传消息日志，请使用控制器GUI界面：

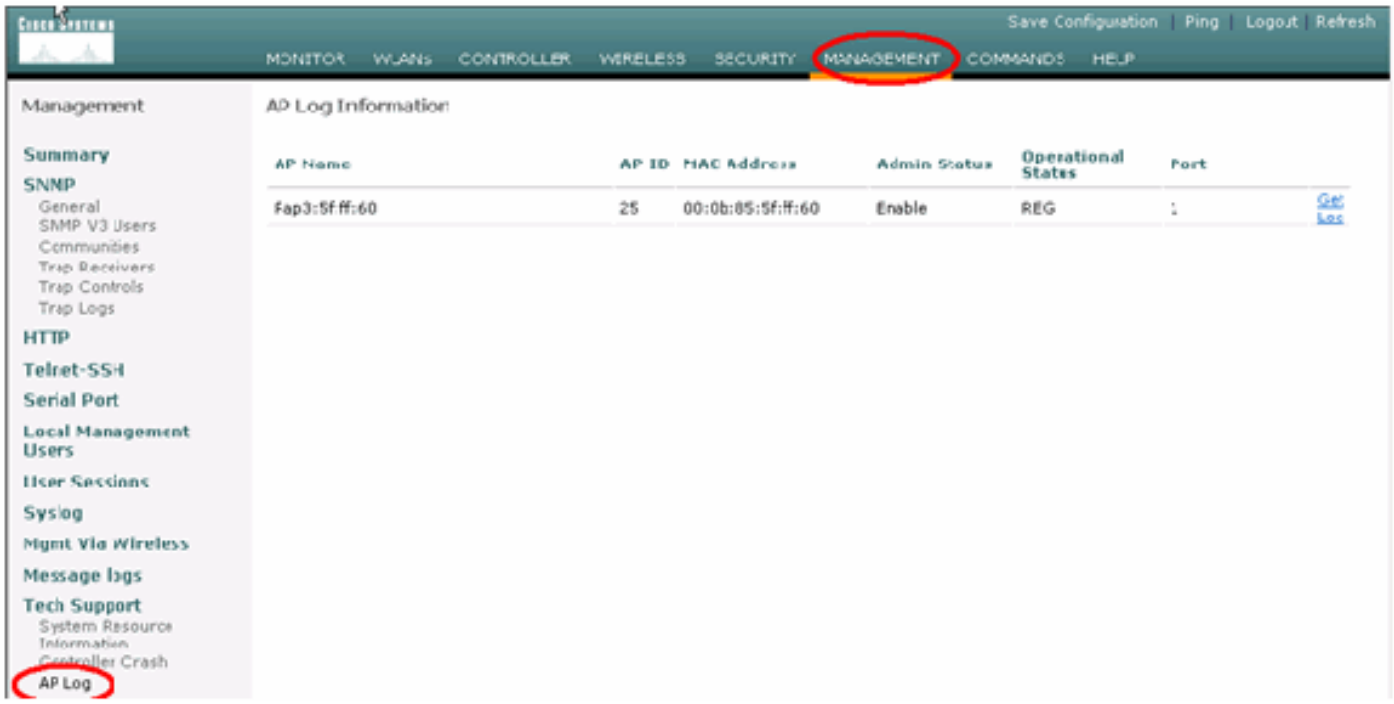
1. 单击“**命令**”> **上传**。



2. 输入TFTP服务器信息。此页面将提供多种上传选项，并且您希望发送这些文件：消息日志事件日志陷阱日志故障文件（如果有）要检查崩溃文件，请单击“管理”>“**控制器崩溃**”。

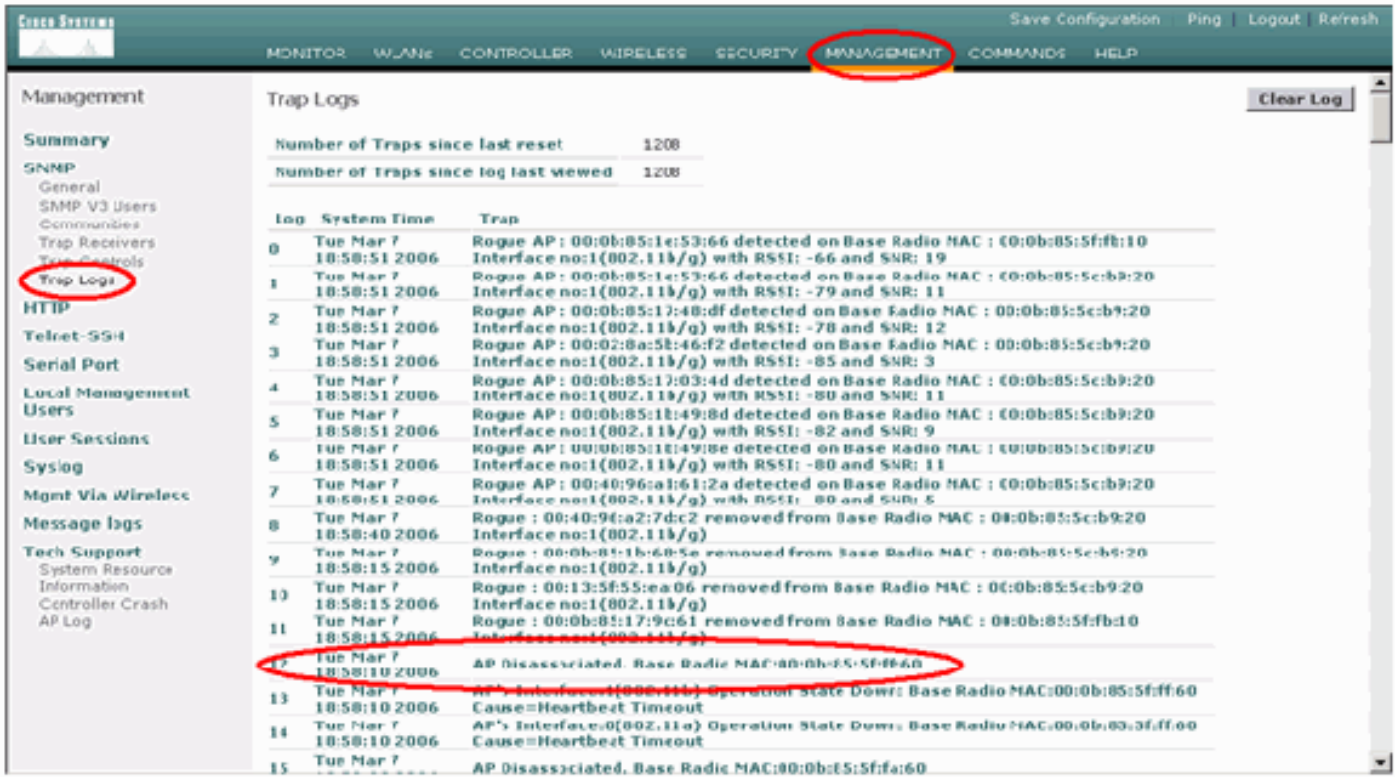
AP日志

转到控制器上的此GUI页面，检查本地AP的AP日志（如果有）：



陷阱日志

转到控制器的此GUI页面并检查陷阱日志：



性能

启动收敛测试

收敛是RAP/MAP与WLAN控制器建立稳定LWAPP连接所花费的时间，从首次启动时开始，如下所列：

收敛测试	**收敛时间（分钟：秒）**			
	RAP	MAP1	MAP2	MAP3
映像升级	2:34	3:50	5:11	6:38
控制器重新启动	0:38	0:57	1:12	1:32
打开室内网状网络	2:44	3:57	5:04	6:09
RAP重启	2:43	3:57	5:04	6:09
MAP重新加入		3:58	5:14	6:25
父级的MAP更改（相同通道）		0:38		

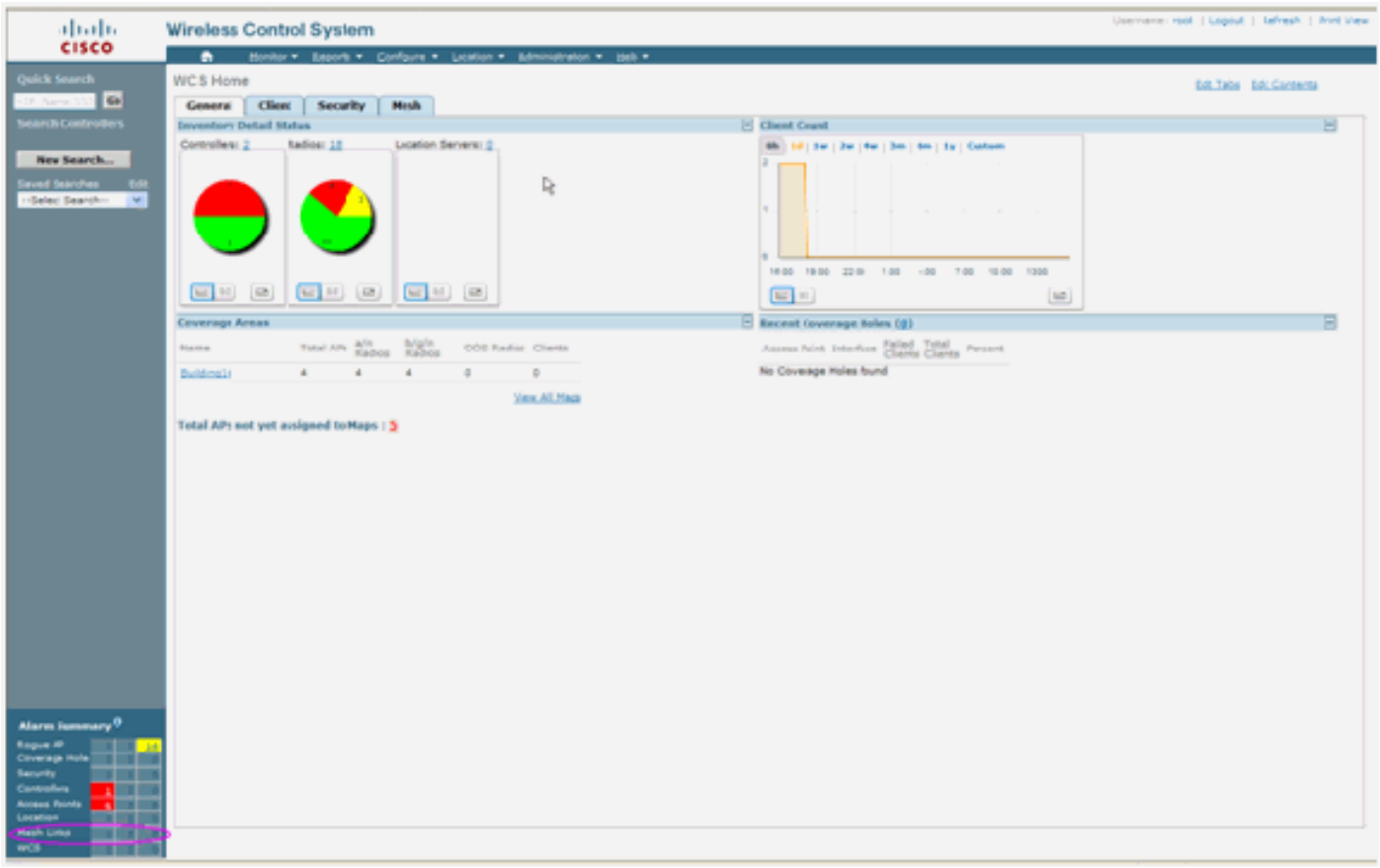
WCS

室内网状警报

WCS将根据来自控制器的陷阱生成与室内网状网络相关的警报和事件：

- 链路SNR低
- 父项已更改
- 子项已移动
- MAP频繁更改父级
- 控制台端口事件
- MAC授权失败
- 验证失败次数
- 子排除父项

单击“网**格链接”**。它将显示与室内网状链路相关的所有警报。



以下警报适用于室内网状链路：

- 链路SNR较差 — 如果链路SNR低于12db，则生成此警报。用户无法更改此阈值。如果在子/父链路的回传链路上检测到SNR不佳，将生成陷阱。陷阱将包含SNR值和MAC地址。警报严重性为严重。SNR（信噪比）比很重要，因为高信号强度不足以保证良好的接收器性能。传入信号必须比存在的任何噪声或干扰强。例如，如果存在强干扰或高噪声级别，则信号强度可能较高，但无线性能仍然较差。
- 父级已更改 — 子级移动到另一父级时生成此警报。当父级丢失时，子级将与另一父级联合，而子级将向WCS发送一个陷阱，其中既包含旧父级地址，也包含新父级的MAC地址。警报严重性：信息.
- 子移动 — 当WCS获取子丢失陷阱时生成此警报。当父AP检测到丢失子AP并且无法与该子AP通信时，它会向WCS发送“丢失子AP”陷阱。陷阱将包含子MAC地址。警报严重性：信息.
- MAP父节点频繁更改 — 如果室内网状AP频繁更改其父节点，则会生成此警报。当MAP parent-change-counter在给定持续时间内超过阈值时，它会向WCS发送陷阱。陷阱将包含MAP更改的次数和时间持续时间。例如，如果2分钟内有5个更改，则陷阱将被发送。警报严重性：信息.
- 子排除父项 — 当子级将父项列入黑名单时生成此警报。当在固定次数的尝试后，子级未能在控制器上进行身份验证时，子级可以将父级列入黑名单。子级会记住列入黑名单的父级，当子级加入网络时，它将发送陷阱，该陷阱包含列入黑名单的父MAC地址和黑名单时间段的持续时间。

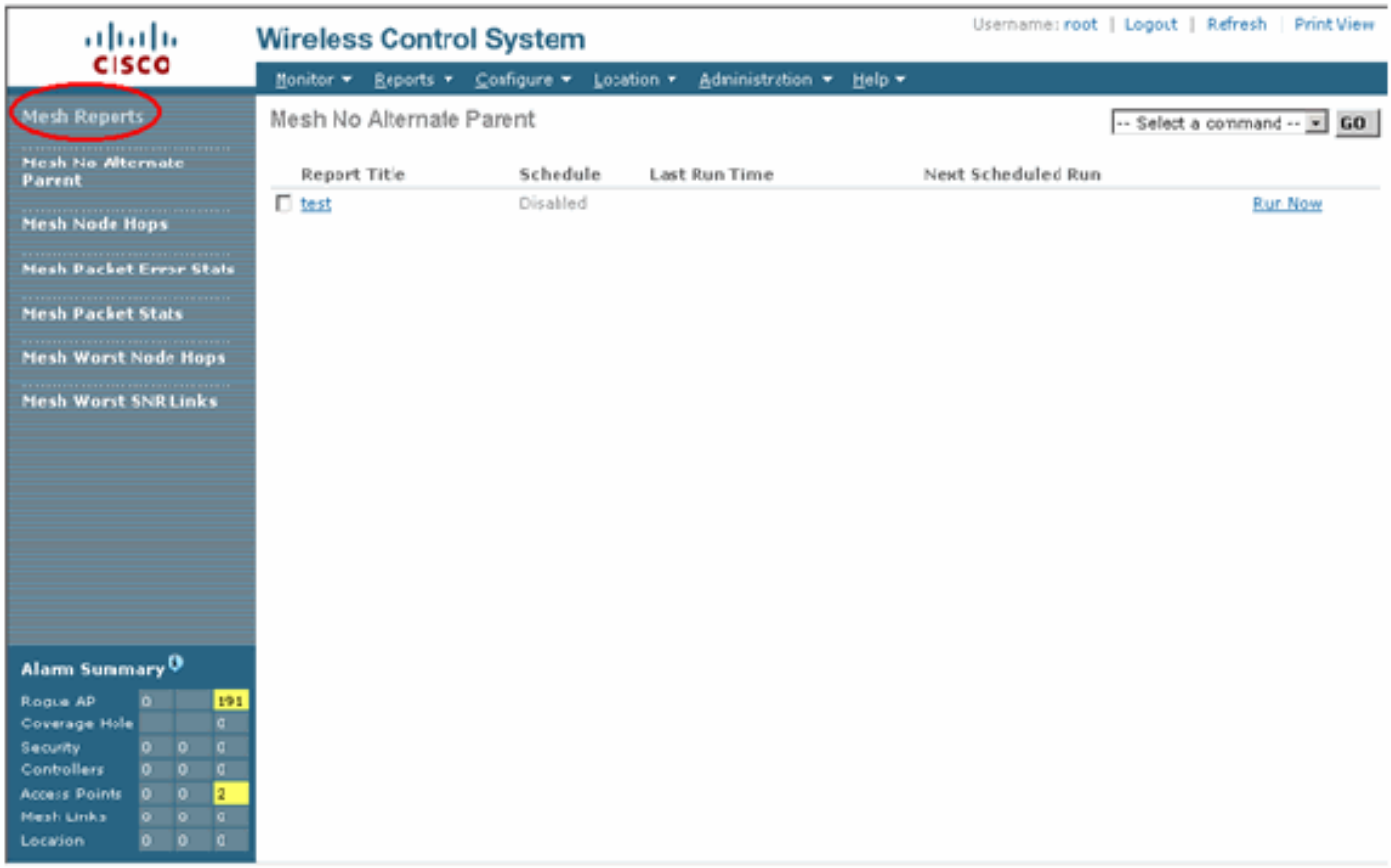
除室内网状链路以外的警报：

- 控制台端口访问 — 控制台端口允许客户更改用户名和密码以恢复滞留的室外AP。但是，为防止任何授权用户访问AP，WCS需要在有人尝试登录时发送警报。由于AP在室外时易受物理攻击，因此需要此警报来提供保护。如果用户成功登录AP控制台端口，或者连续三次失败，将生成此警报。
- MAC授权失败 — 当AP尝试加入室内网状网但由于未在MAC过滤器列表中而无法进行身份验证时，会生成此警报。WCS将从控制器接收陷阱。陷阱将包含授权失败的AP的MAC地址。

网状报告和统计信息

我们从4.1.185.0开始执行增强的报告和统计框架：

- 无备用路径
- 网状节点跳数
- 数据包错误统计信息
- 数据包统计信息
- 最差节点跳
- 最差SNR链路



无备用路径

室内网状AP通常有多个邻居。如果室内网状AP丢失其父链路，则AP应能找到备用父链路。在某些情况下，如果没有显示邻居，则AP如果失去其父级，将无法访问其他父级。用户必须知道哪些AP没有备用父级。此报告列出除当前父交换机之外没有任何其他邻居的所有AP。

室内网状节点跳数

此报告显示离根AP(RAP)的跳数。 您可以根据以下条件创建报告：

- 按控制器划分的AP
- 按楼层划分的AP

数据包错误率

数据包错误可能是由干扰和丢包引起的。数据包错误率计算基于发送的数据包和成功发送的数据包

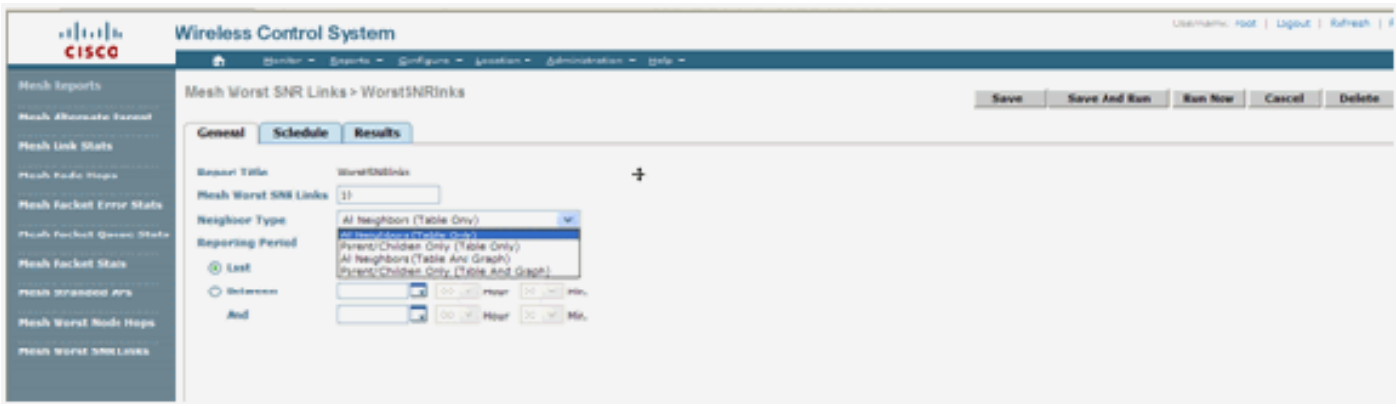
。数据包错误率在回传链路上测量，并为邻居和父链路收集。AP定期向控制器发送数据包信息。一旦父交换机发生更改，AP就会将收集到的数据包错误信息发送到控制器。默认情况下，WCS每10分钟从控制器轮询一次数据包错误信息，并将其存储在数据库中长达7天。在WCS中，数据包错误率显示为图形。数据包错误图基于数据库中存储的历史数据。

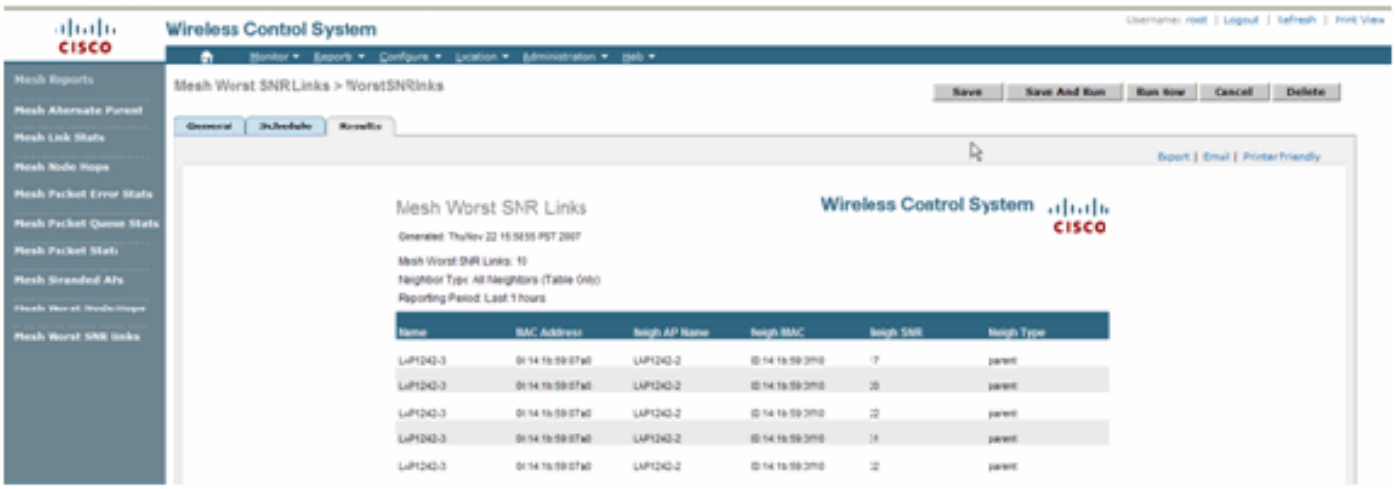
数据包统计信息

此报告显示邻居总传输数据包和成功传输的邻居总数据包的计数器值。您可以根据某些条件创建报告。

最差SNR链路

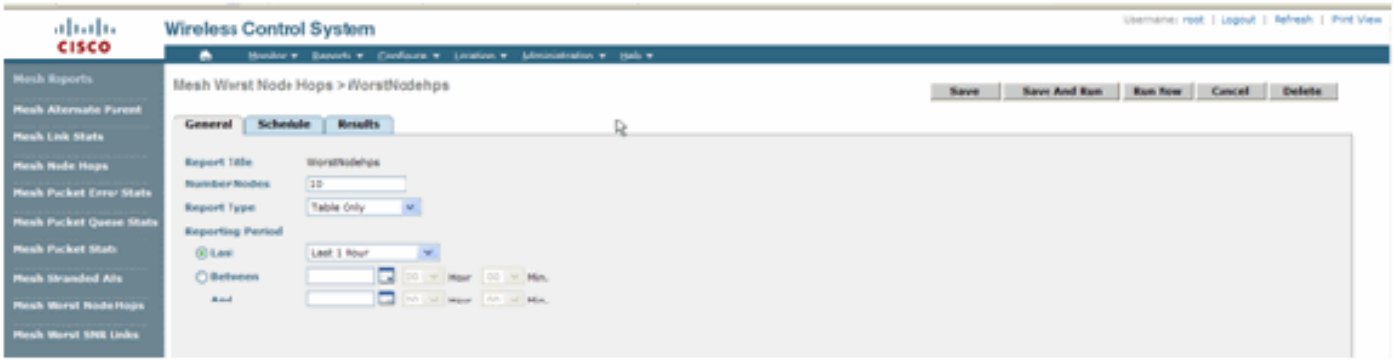
噪音问题可能发生在不同的时间，噪音可能以不同的速率增加或持续不同的时间。下图提供了为无线电a和b/g以及选择性接口创建报告的功能。默认情况下，报告列出10条最差SNR链路。您可以选择5到50个最差的链路。报告可以生成为过去1小时、过去6小时、最后一天、过去2天和最多7天。默认情况下，每10分钟轮询一次数据。数据最多保存在数据库中七天。邻居类型选择条件可以是所有邻居，仅父/子。



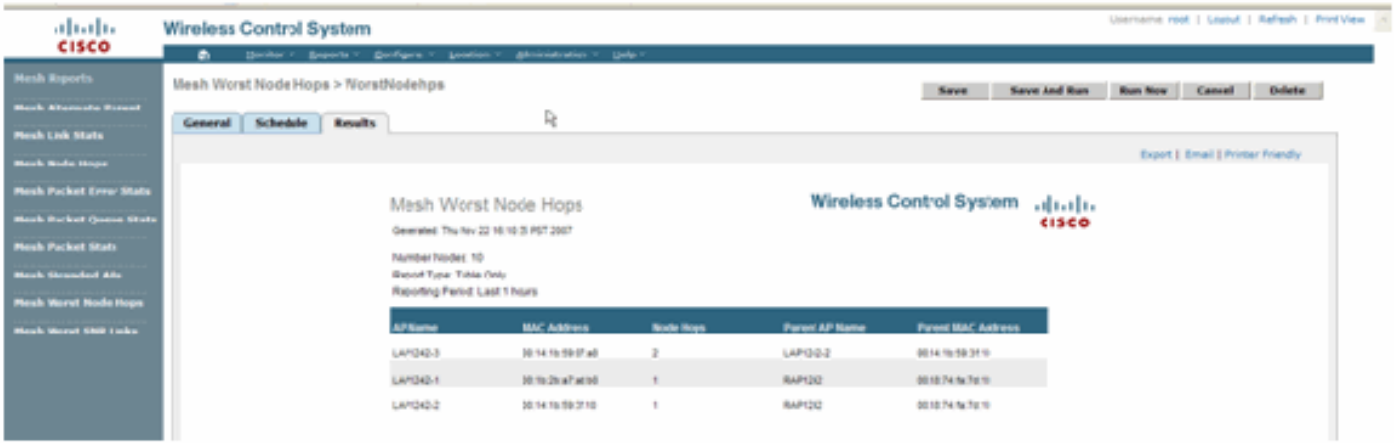


最差节点跳数

此报告列出了默认情况下10个最差跳AP。如果AP的跳数过多，链路可能非常薄弱。用户可以隔离与根AP相距多跳的AP，并采取相应措施。您可以选择将此节**点数标**准更改为5到50。此图中**的"报**表类型"筛选标准可以是"仅表"或"表和图形"：



此图显示了上次报告的结果：



安全统计

室内网状网安全统计信息显示在AP详细信息页面的桥接信息部分下。当子室内网状节点与父室内网状节点关联或进行身份验证时，会创建室内网状节点安全统计信息表中的条目。当室内网状网节点与控制器取消关联时，将删除条目。

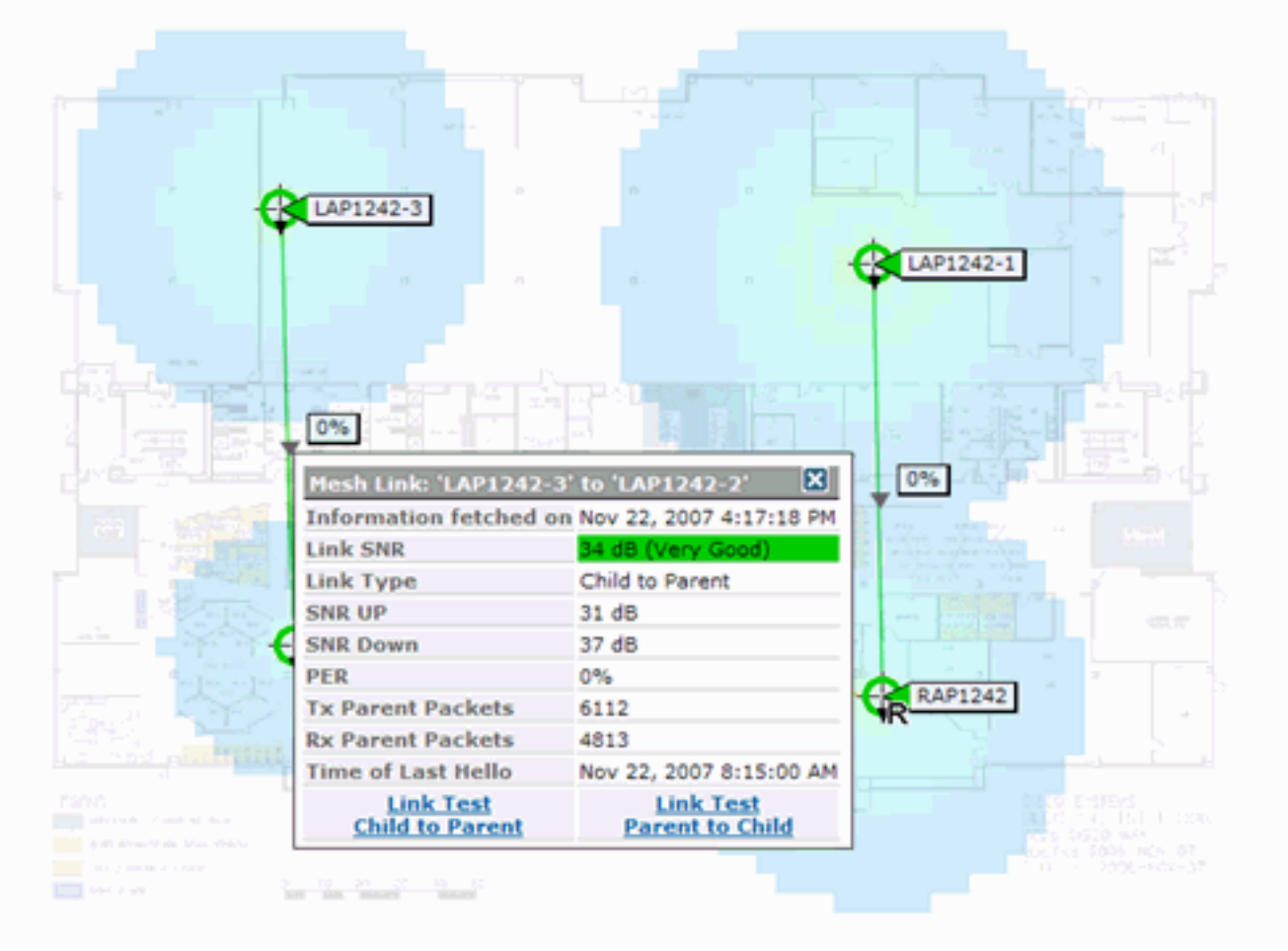
链路测试

WCS支持AP到AP链路测试。您可以选择任意两个AP，并在两个AP之间调用链路测试。

如果这些AP是RF邻居，则链路测试可能会产生结果。结果显示在映射本身的对话框中，没有完整的页面刷新。该对话可以容易地处理。

但是，如果这2个AP不是RF邻居，则WCS不会尝试找出2个AP之间的路径，以便进行组合多链路测试。

当鼠标移动到两个节点之间链路上的箭头上时，将显示此窗口：



节点到节点链路测试

链路测试工具是用于验证任意两个AP之间链路质量的按需工具。在WCS中，此功能会添加到AP详细信息页面。

在AP详细信息页面的“室内网状**链路”(Indoor Mesh Link)**选项卡下，其旁边列有链路，其中有一个用于执行链路测试的链接。

控制器CLI链接测试工具具有可选的输入参数：数据包大小、总链路测试数据包、测试持续时间和数据链路速率。链路测试具有这些可选参数的默认值。节点的MAC地址是唯一必需的输入参数。

链路测试工具测试节点之间发送的数据包和收到的数据包的强度。链路测试的链接显示在AP详细信息报告中。单击链接时，会弹出一个屏幕，显示链接测试结果。链路测试仅适用于父子节点和邻居之间。

链路测试输出会生成发送的数据包、接收的数据包、错误数据包（因差异原因而存在的桶）、SNR、噪声楼层和RSSI。

链路测试至少在GUI上提供以下详细信息：

- 发送的链路测试数据包
- 收到的链路测试数据包
- 信号强度（以dBm为单位）
- 信噪比

按需AP邻居链路

这是WCS映射中的一项新功能。您可以点击网状AP，并显示一个包含详细信息的弹出窗口。然后，可单击**View Mesh Neighbors**，该选项将获取所选AP的邻居信息，并显示包含所选室内网状AP的所有邻居的表。

查看网状邻居链路显示突出显示的AP的所有邻居。此快照显示所有邻居、邻居的类型和SNR值。

Ping 测试

Ping测试是一种按需工具，用于在控制器和AP之间执行ping操作。Ping测试工具在AP详细信息页面和MAP中都可用。在AP详细信息页**面或从MAP AP信息中单击Run Ping Test（运行Ping测试）链接**，以启动从控制器到当前AP的ping操作。

结论

企业网状网（即室内网状网）是思科无线覆盖范围的延伸，扩展至有线以太网无法提供连接的地方。无线网络的灵活性和可管理性可通过企业网状网实现。

有线AP提供的大多数功能都由室内网状拓扑提供。企业网状网也可以与同一控制器上的有线AP共存。

相关信息

- 技术支持和文档 - Cisco Systems