室內網狀部署指南

目錄

簡介

輕量型接入點1242/1131是用於選定室內部署的雙無線電Wi-Fi基礎設施裝置。它是一種基於輕量型存取點通訊協定(LWAPP)的產品。它提供2.4 GHz無線電和5.8 GHz無線電與802.11b/g和802.11a相容。一個無線電可用於接入點(AP)的本地（客戶端）接入，第二個無線電可用於無線回傳。LAP1242/LAP1131支援P2P、P2MP和網狀架構。

嘗試任何安裝之前，請務必通讀指南。

本文檔介紹用於室內網狀網路的企業無線網狀網路的部署。本文檔將使無線終端使用者瞭解室內網狀網的基本原理、在何處配置室內網狀網以及如何配置室內網狀網。室內網狀網路是使用無線控制器和輕量AP部署的Cisco企業無線網狀網路的子集。

室內網狀網是在統一無線架構上部署的企業網狀架構的子集。現今對室內網狀網路的需求很大。使用室內網狀網時，其中一個無線電（通常為802.11b/g）和/或有線乙太網鏈路用於連線客戶端，而第二個無線電（通常為802.11a）用於回傳客戶端流量。回傳可以是單跳或多跳。室內網狀網路為您提供以下值：

- 無需為每個AP運行乙太網佈線。
- 每個AP不需要乙太網交換機埠。
- 網路連線，其中線路無法提供連線。
- 部署靈活性 — 不限於乙太網交換機的100米。
- 易於部署點對點無線網路。

由於佈線成本節省以及前面提到的原因，大型機箱零售商對室內網狀網非常感興趣。

庫存專家使用它來清點零售商、製造工廠和其他公司的庫存。他們希望快速在客戶站點部署臨時Wi-Fi網路，以便為手持裝置提供即時連線。教育研討會、會議、製造和招待是需要室內網狀架構的一些地方。

閱讀完本指南後，您將瞭解使用何處和如何配置室內網狀。您還將瞭解，NEMA機箱中的室內網狀不能替代室外網狀。此外，您還將瞭解室內MAP相對於自治AP使用的鏈路角色靈活性（單跳網路）的優勢。

假設：

您已瞭解思科統一無線網路、架構和產品。您已瞭解思科室外網狀網產品和網狀網網路使用的某些術語。

縮寫詞術語表	
LWAPP	輕量型存取點通訊協定 — AP與無線LAN控制器之間的控制和資料通道通訊協定。
WLAN控制器/控制器/WLC	無線LAN控制器 — 思科裝置，通過將大量受管端點合併到單個統一系統中，集中並簡化WLAN的網路管理

	，從而支援統一智慧資訊WLAN網路系統。
RAP	根接入點/屋頂接入點 — 思科無線裝置充當控制器和其他無線AP之間的橋樑。連線到控制器的AP。
地圖	網狀AP — 思科無線裝置，通過802.11a無線電上的RAP或MAP無線連線，同時為802.11b/g無線電上的客戶端提供服務。
父項	一種AP(RAP/MAP)，用於通過802.11a無線電提供對其他AP的無線訪問。
鄰居	網狀網路中的所有AP都是鄰居且具有鄰居。RAP沒有鄰居，因為它連線到控制器。
兒童	遠離控制器的AP始終是子級。一個子節點在網狀網路中有一個父節點和多個鄰居。如果父項死亡，則選擇具有最佳緩動值的下一個鄰居。
SNR	訊雜比
BGN	網橋組名稱
EAP	可擴充驗證通訊協定
PSK	預共用金鑰
AWPP	調適型無線路徑通訊協定

概觀

思科室內網狀網路接入點是用於選定室內部署的雙無線電Wi-Fi基礎設施裝置。它是一種基於輕量型存取點通訊協定(LWAPP)的產品。它提供與802.11b/g、802.11a標準相容的2.4 GHz無線電和5.8 GHz無線電功能。一個無線電(802.11b/g)可用於AP的本地（客戶端）接入，第二個無線電(802.11a)可配置用於無線回傳。它提供室內網狀架構，不同節點（無線電）通過回傳相互通訊，並提供本地客戶端訪問。此AP還可用於點對點和點對多點橋接架構。無線室內網狀網路解決方案非常適合大型室內覆蓋範圍，因為您可以使用最低的基礎架構實現高資料速率和良好的可靠性。以下是該產品首次發佈時引入的基本突出功能：

- 在室內環境中用於3跳數。最多4個。
- 終端使用者客戶端的中繼節點和主機。802.11a無線電用作回傳介面，802.11b/g無線電用於服務客戶端。
- 室內網狀AP安全 — 支援EAP和PSK。
- 網狀環境中的LWAPP MAP與控制器的通訊方式與乙太網連線的AP相同。
- 點對點無線橋接。
- 點對多點無線橋接。
- 最佳父項選擇。SNR、EASE和BGN
- BGN增強功能。NULL和預設模式。
- 本地訪問。

- 父黑名單。排除清單。
- 使用AWPP進行自我修復。
- 乙太網路橋接。
- 對4.0版本語音的基本支援。
- 動態頻率選擇。
- 反串流 — 預設BGN和DHCP故障切換。

注意：這些功能不受支援：

- 4.9 GHz公共安全通道
- 干擾路由
- 後台掃描
- 通用訪問
- 工作組網橋支援

室內網狀軟體

室內網狀軟體是一個特殊的版本，因為它集中於室內AP，特別是室內網狀網路。在此版本中，我們的室內AP都在本地模式下工作，也都在網橋模式下工作。4.1.171.0版本中提供的某些功能在此版本中未實現。對命令列介面(CLI)、圖形使用者介面（GUI - web瀏覽器）以及狀態機本身進行了改進。這些改進的目的在於從您的角度獲得有關新產品及其功能可行性的寶貴資訊。

室內網狀網特定增強功能：

- **室內環**境 — 使用LAP1242s和LAP1131實現室內網狀。在沒有乙太網電纜的室內環境中實現室內網狀。實施過程簡單且快速，可為建築物內的偏遠地區（例如，零售配送中心、研討會/會議教育、製造、酒店）提供無線覆蓋。
- **網橋組名稱(BGN)增強功**能 — 為了允許網路管理員將室內網狀存取點網路組織到使用者指定的區段，思科提供了一種稱為網橋組名稱(BGN)的機制。BGN（其實是扇區名稱）導致AP連線到具有相同BGN的其他AP。如果AP找不到與其BGN匹配的合適扇區，則AP在預設模式下運行，並選擇對預設BGN作出響應的最佳父級。在應對擱淺的AP條件（如果有人錯誤配置了BGN）時，該功能已經得到了現場的廣泛讚譽。 在4.1.171.0軟體版本中，使用預設BGN時，AP不作為室內網狀節點運行，並且沒有任何客戶端訪問。通過控制器進行訪問時處於維護模式，如果管理員沒有修復BGN，AP將在30分鐘後重新啟動。
- **安全增強**功能 — 室內網狀網代碼上的安全預設配置為EAP（可擴展身份驗證協定）。RFC3748中對此進行了定義。雖然EAP協定不限於無線LAN並且可用於有線LAN身份驗證，但它最常用於無線LAN。當啟用了802.1X的NAS（網路訪問伺服器）裝置（例如802.11 a/b/g無線接入點）呼叫EAP時，現代EAP方法可以提供安全的身份驗證機制，並在客戶端和NAS之間協商安全的PMK（成對主金鑰）。然後，PMK可用於使用TKIP或CCMP（基於AES）加密的無線加密會話。在4.1.171.0軟體版本之前，室外網狀AP使用PMK/BMK加入控制器。這是一個三週期的過程。現在，為了加快收斂速度，週期被縮短。室內網狀網路安全的總體目標是提供：零接觸配置用於調配安全性。資料幀的隱私和身份驗證。網路和節點之間的相互身份驗證。能夠使用標準EAP方法對室內網狀AP節點進行身份驗證。分離LWAPP和室內網狀安全。發現、路由和同步機制從當前架構得到增強，以適應支援新安全協定所需的元素。室內網狀AP通過掃描和偵聽來自其他網狀AP的無償鄰居更新來發現其他網狀AP。連線到網路的任何RAP或室內MAP都會在其NEIGH_UPD幀中通告核心安全引數（非常類似於802.11信標幀）。此階段結束後，室內網狀AP和根AP之間建立邏輯鏈路。
- **WCS增強功能**已新增室內網狀警報。可以生成顯示跳數、最差SNR等的室內網狀報告。可以在節點之間運行連結測試（父到子、子到父），顯示非常智慧的資訊。顯示的AP資訊比之前的資訊多得多。你還可以選擇檢視潛在的鄰居。改進了運行狀況監控，並且更便於訪問。

支援的硬體和軟體

室內網狀網路的最低硬體和軟體要求：

- Cisco LWAPP AP AIR-LAP1242AG-A-K9和AIR-LAP1131AG-A-K9支援室內網狀配置。
- Cisco Mesh Release 2軟體支援Enterprise Mesh（室內和室外產品）。 只能安裝在思科控制器、Cisco 440x/210x和WISM上。
- Cisco Enterprise Mesh Release 2軟體可從Cisco.com下載。

室內與室外

以下是室內和室外網狀網之間的一些顯著差異：

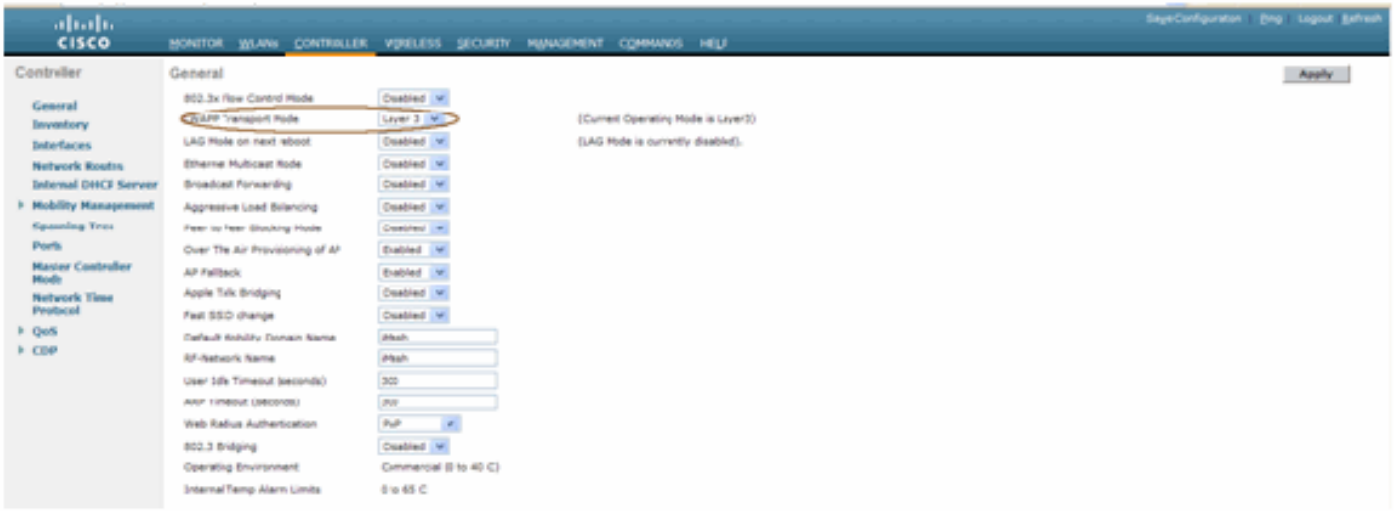
	室內網狀	室外網狀
環境	僅限室內，硬體為室內評級	僅用於室外，堅固型硬體
硬體	使用LAP1242和LAP1131AG的室內AP	使用LAP15xx和LAP152x的室外AP
電源級別	2.4 Ghz:20dbm 5.8 Ghz:17dbm	2.4 Ghz:28dbm 5.8 Ghz:28dbm
單元格大小	約150英尺	約1000英尺
實現高度	離地面12英尺	離地面30-40英尺

組態

在開始任何實施之前，尤其當您收到新硬體時，請務必仔細閱讀指南。

控制器L3模式

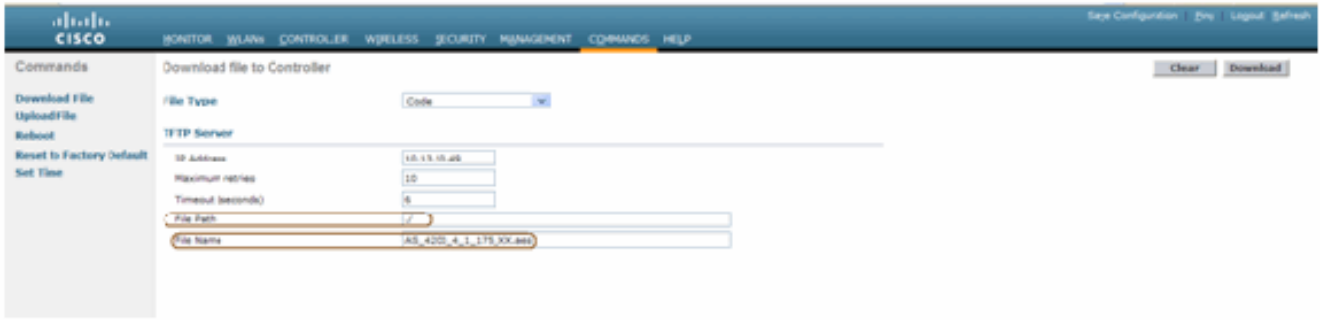
室內網狀AP可以部署為L3網路。



將控制器升級為最新代碼

請完成以下步驟：

1. 要在室內網狀網路上升級網狀版本2，您的網路必須在4.1.185.0或Mesh Release1上運行(可從Cisco.com獲得)。
2. 將控制器的最新代碼下載到TFTP伺服器。在控制器GUI介面中，按一下「**Commands**」>「**Download file**」。
3. 選擇File type as **code**，並指定TFTP伺服器的IP地址。定義檔案的路徑和名稱。



注意：使用支援超過32 MB檔案大小傳輸的TFTP伺服器。例如，**tftpd32**。在File path put **"./"下，如**所示。

4. 安裝完新韌體後，在CLI中使用**show sysinfo**命令驗證是否已安裝新韌體。

```
(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：在官方層面，思科不支援控制器降級。

MAC 地址

必須使用MAC過濾。此功能使思科室內網狀解決方案成為真正的「零接觸」。 與先前版本不同，網狀螢幕將不再具有MAC過濾選項。

注意：預設情況下啟用MAC過濾。

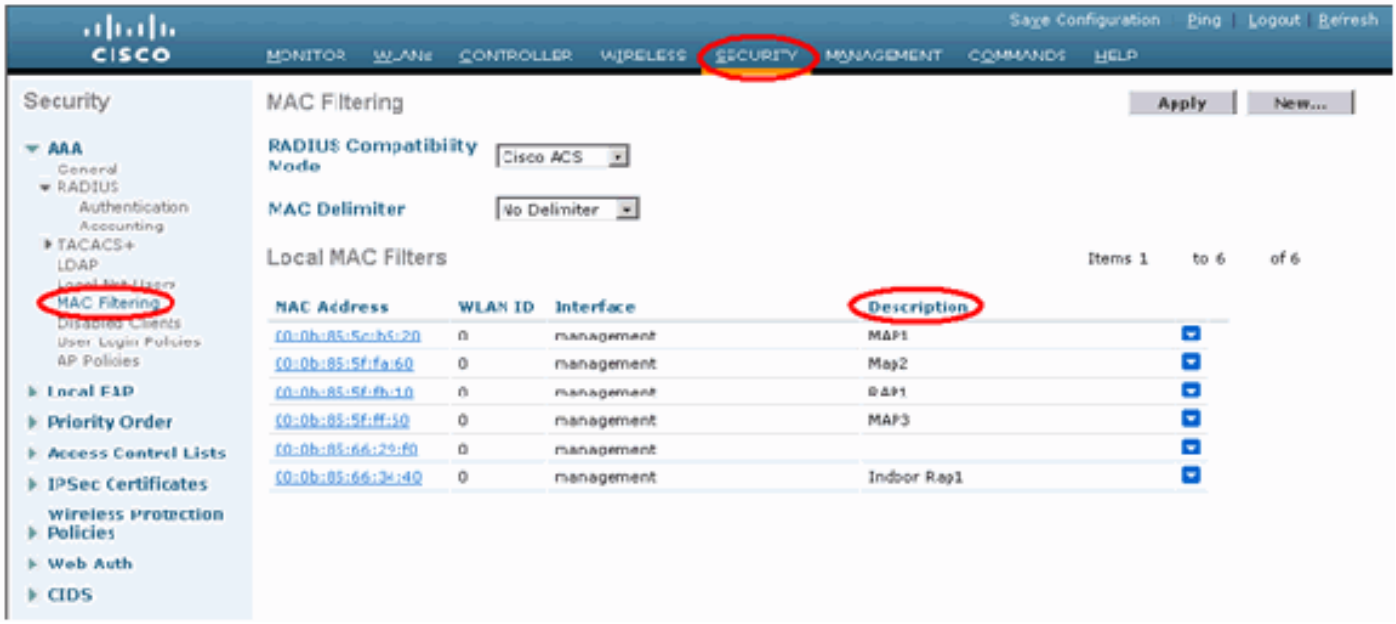
記錄無線電的MAC地址

在文本檔案中，記錄您在網路中部署的所有室內網狀AP無線電的MAC地址。MAC地址可以在AP的背面找到。這有助於您進行將來的測試，因為大多數CLI命令都要求使用該命令輸入AP的MAC地址或名稱。您還可以將AP的名稱更改為更易於記住的名稱，例如「building number-pod number-AP type:最後四個MAC地址十六進位制字元。"

輸入控制器中的MAC地址和無線電名稱

思科控制器維護室內AP授權MAC地址清單。控制器僅對授權清單中顯示的室內無線電的發現請求做出響應。輸入控制器上網路中要使用的所有無線電的MAC地址。

在控制器GUI介面上，轉到**Security**，然後按一下螢幕左側的**MAC filtering**。按一下**New**以輸入MAC位址，如下所示：



此外，為了方便起見，請在**說明**下輸入無線電的名稱（如位置、AP號等）說明還可用於安裝無線電的位置，以便隨時參考。

啟用MAC過濾

預設情況下啟用MAC過濾。

也可以在同一頁面上選擇安全模式為EAP或PSK。

在交換器的GUI介面中，使用以下路徑：

GUI介面路徑：**無線>室內網狀**

只能使用以下命令在CLI上檢查安全模式：

```
(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
```

第3層室內網狀部署

對於L3室內網狀網路，如果您不打算使用DHCP伺服器（內部或外部），請配置無線電的IP地址。

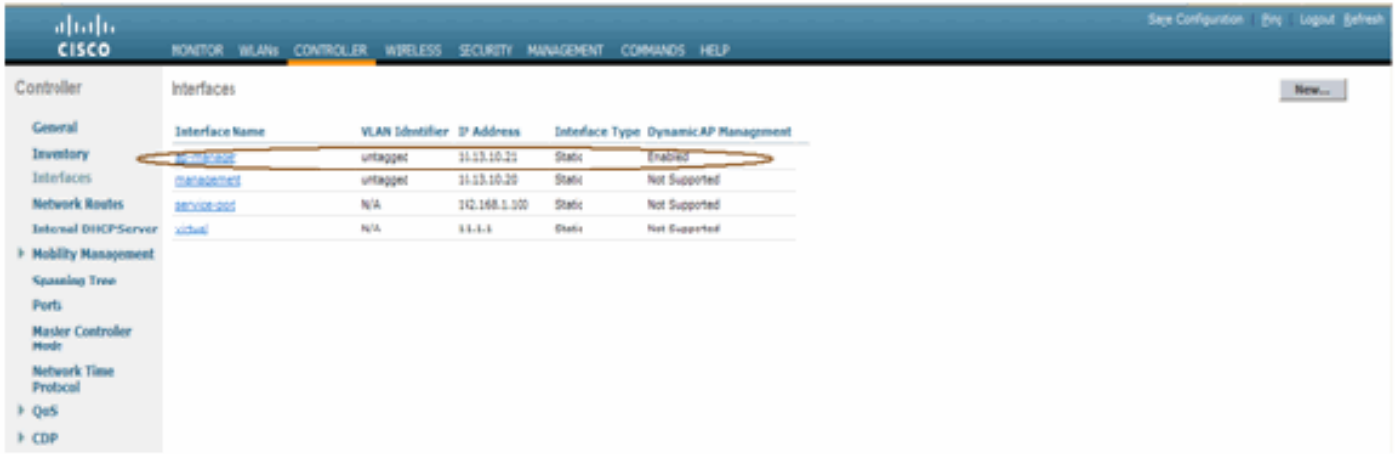
對於L3室內網狀網路，如果要使用DHCP伺服器，請在L3模式下配置控制器。儲存組態並重新啟動控制器。確保在DHCP伺服器上配置選項43。控制器重新啟動後，新連線的AP將從DHCP伺服器接收其IP地址。

定義控制器上的介面

AP管理器

對於L3部署，必須定義**AP-manager**。AP管理器用作從控制器到AP通訊的源IP地址。

路徑：**Controller > Interfaces > ap-manager > edit**。



應該為**AP-manager**介面分配與管理介面相同的子網和VLAN中的IP地址。

無線電角色

此解決方案可能具有兩個主要無線電角色：

- 根接入點(RAP) — 要用於連線到控制器（通過交換機）的無線電將充當RAP的角色。RAP與控制器之間具有支援LWAPP的有線連線。RAP是任何橋接或室內網狀網路的父節點。一個控制器可以有一個或多個RAP，每個一個RAP提供相同或不同的無線網路。同一室內網狀網路可以有多個用於冗餘的RAP。
- 室內網狀無線接入點(MAP) — 與控制器沒有有線連線的無線電充當室內網狀無線接入點。此AP以前稱為Pole top AP。MAP具有到其他MAP（最後到RAP，進而到控制器）的無線連線（通過回傳介面）。MAP還可以具有到LAN的有線乙太網連線，並用作該LAN的橋接端點（使用P2P或P2MP連線）。 如果正確配置為乙太網網橋，則可能同時發生這種情況。MAP為不用於回程介面的頻段上的客戶端提供服務。

AP的預設模式是MAP。

注意：可以通過GUI或CLI設定無線電角色。角色更改後，AP將重新啟動。

注意：如果AP以物理方式連線到交換機，或者您能看到交換機上的AP作為RAP或MAP，則可以使用控制器CLI在AP上預配置無線電角色。

```
(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)
```

網橋組名稱

網橋組名稱(BGN)控制AP的關聯。BGN可以對無線電進行邏輯分組，以避免同一通道上的兩個網路相互通訊。如果同一扇區（區域）中的網路中有多個RAP，此設定也很有用。 BGN是一個最多包含10個字元的字串。

工廠設定的網橋組名稱在生產階段分配(NULL VALUE)。 您看不到它。因此，即使沒有定義的BGN，無線電仍然可以加入網路。如果您的網路在同一扇區中有兩個RAP（為了獲得更大的容量），建議您使用相同的BGN但在不同的通道上配置兩個RAP。

注意：可以從控制器CLI和GUI設定網橋組名稱。

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

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

配置BGN後，AP將重置。

注意：應在即時網路上非常謹慎地配置BGN。您應該始終從最遠的節點（最後一個節點）開始，並向RAP移動。原因是，如果您開始在多重躍點中間的某個位置配置BGN，則超過此點的節點將被丟棄，因為這些節點將具有不同的BGN（舊BGN）。

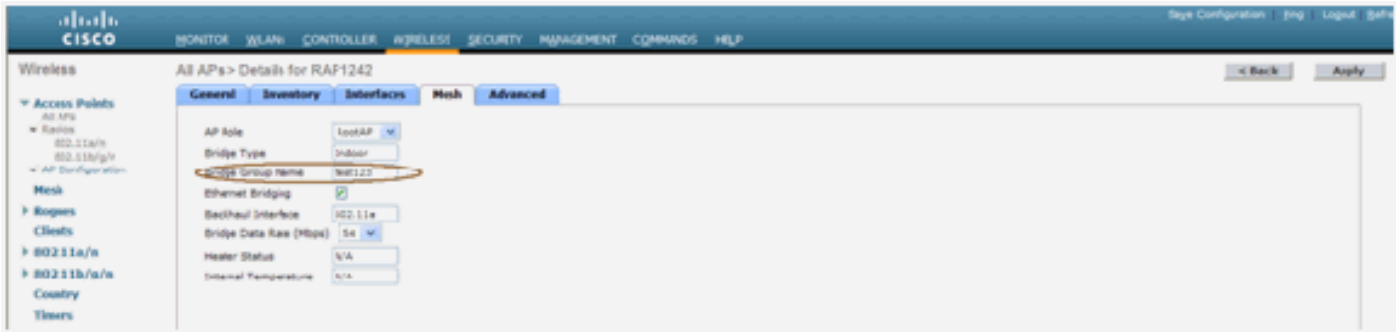
您可以通過發出以下CLI命令驗證BGN:

(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，您還可以使用控制器GUI設定或驗證BGN:

路徑：**Wireless > All APs > Details**。



您可以看到，此新版本還會顯示AP的環境資訊。

安全配置

預設室內網狀安全模式為EAP。這表示除非在控制器上設定這些引數，否則您的MAP不會加入：

室內網狀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.
```

如果您需要一直處於PSK模式，請使用以下命令返回到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
```

室內網狀EAP show命令

在EAP模式下，您可以檢查以下**show**命令以驗證MAP身份驗證：

```
(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
```

室內網狀EAP debug命令

若要偵錯任何EAP模式問題，請在控制器中使用以下命令：

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

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

安裝

前提條件

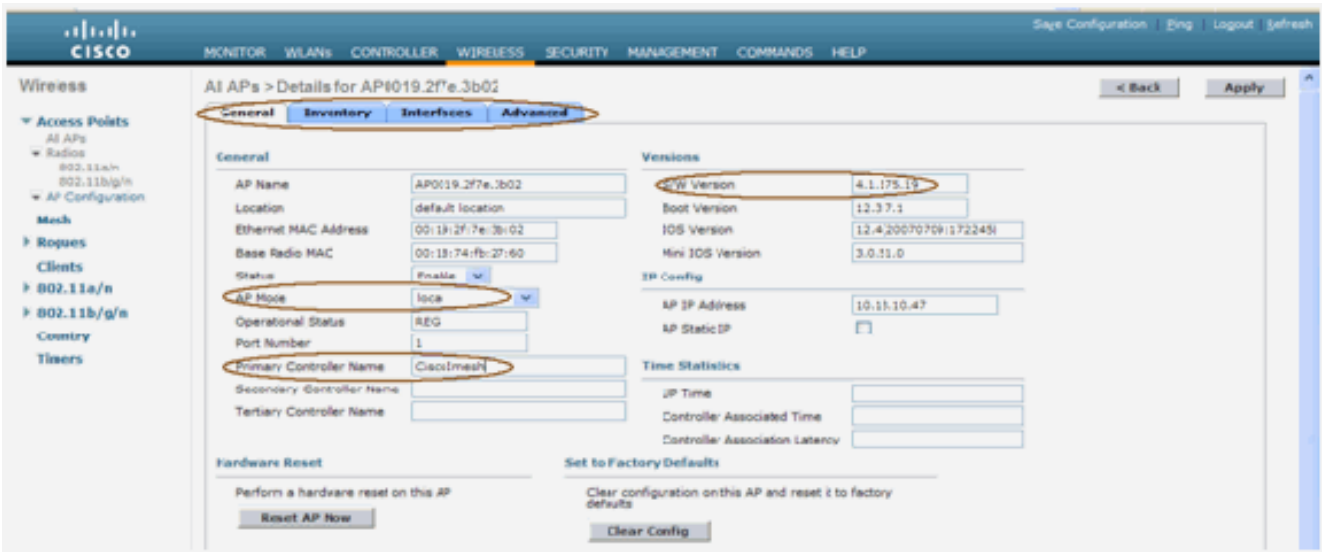
控制器必須運行推薦版本的代碼。按一下「Monitor」以驗證軟體版本。也可通過CLI進行驗證。

```
(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
```

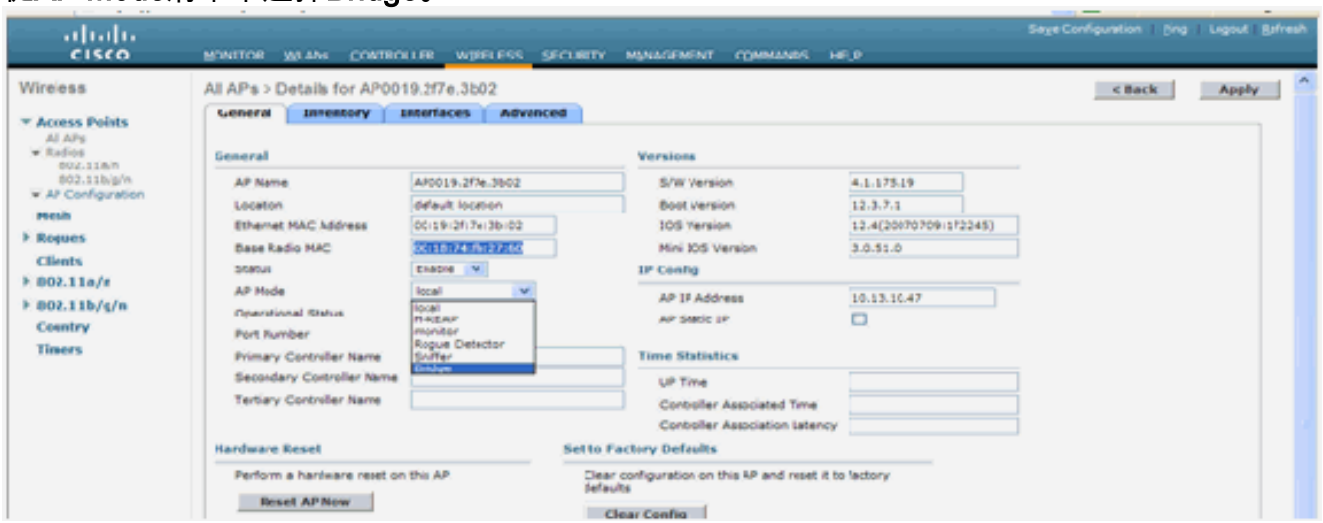
應可以訪問DHCP伺服器、ACS伺服器和WCS伺服器等系統。

安裝

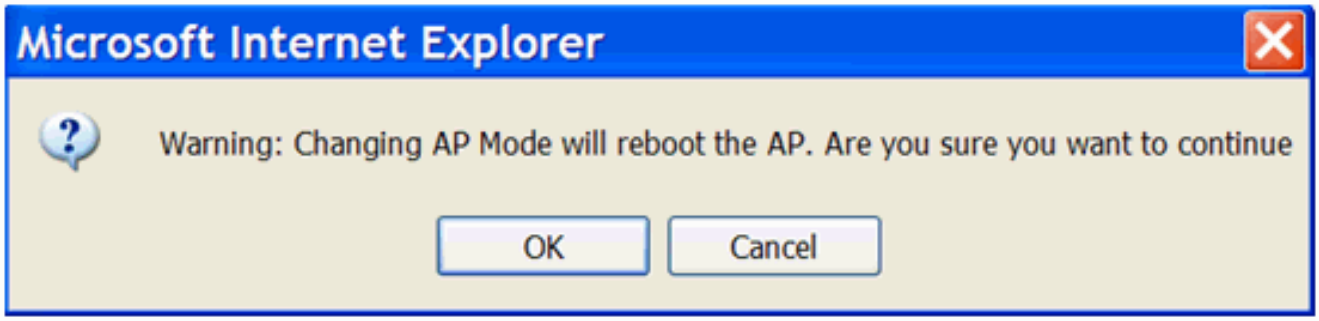
1. 將所有LAP(1131AG/1242AG)連線到與管理IP地址位於同一子網的第3層網路。所有AP將作為本地模式下的AP加入控制器。在此模式下，使用主控制器名稱、輔助控制器名稱和第三控制器名稱來初始化AP。



2. 捕獲AP的基本無線電MAC地址(例如，00:18:74:fb:27:60）。
3. 新增AP的MAC地址以使AP在網橋模式下加入。
4. 按一下「**Security**」>「**MAC-filtering**」>「**New**」。
5. 新增複製的MAC地址，並在MAC過濾器清單和AP清單中命名AP。
6. 從**AP Mode**清單中選擇**Bridge**。



7. 它會提示您確認此操作將重新啟動AP。



8. AP將重新啟動並以橋接模式加入控制器。新的AP視窗將有一個額外的頁籤：網狀。按一下**MESH**頁籤驗證角色、網橋型別、網橋組名稱、乙太網橋接、回程介面、網橋資料速率等。

9. 在此視窗中，訪問AP角色清單並選擇相關角色。在這種情況下，角色預設為MAP。預設情況下，網橋組名稱為空。回程介面是802.11a。網橋資料速率（即回程資料速率）為24 Mbps。
10. 將您想要作為RAP的AP連線到控制器。在所需位置部署無線電(MAP)。開啟收音機。您應該可以看到控制器上的所有無線電。

```
(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. 嘗試在節點之間設定視線條件。如果視線條件不存在，請建立菲涅耳區域間隙以獲得近距離視線條件。
12. 如果有多個控制器連線到同一個室內網狀網路，則必須在每個節點上指定主控制器的名稱。否則，首先看到的控制器將作為主控制器。

電源和通道配置

回傳通道可在RAP上配置。MAP將調整到RAP通道。可以為MAP單獨配置本地訪問。

在交換器GUI上，依照路徑：**Wireless > 802.11a radio > configure**。

注意：回傳上的預設Tx功率級別是最高功率級別（級別1），無線電資源管理(RRM)預設處於關閉狀態。

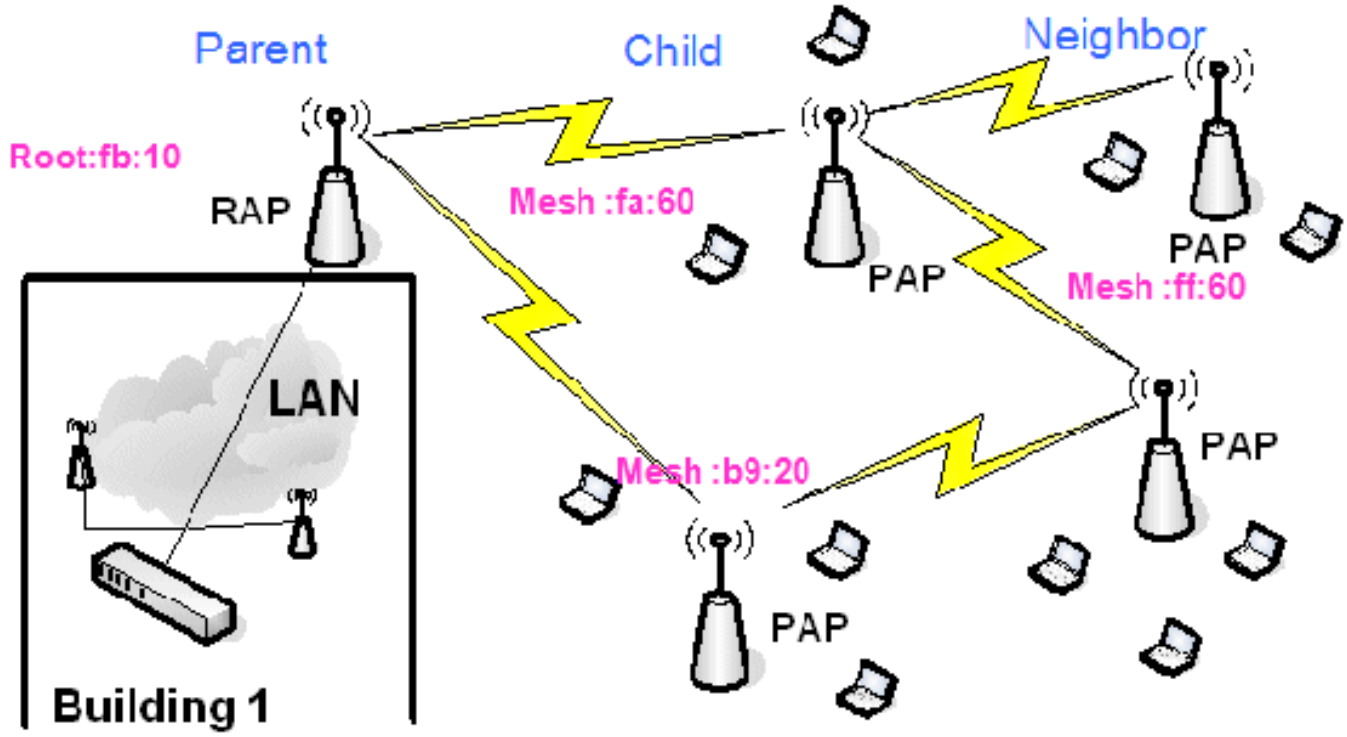
如果您要配置RAP，我們建議您在每個RAP上使用備用相鄰通道。這將減少同通道干擾。

RF檢查

在室內網狀網路中，必須驗證節點之間的父子關係。Hop是兩個無線電之間的無線鏈路。父子關係隨您通過網路傳輸而變化。這取決於您在室內網狀網路中的位置。

在無線連線（躍點）中，距離控制器較近的無線電是**躍點另一端**無線電的Parent。在多跳系統中，有一個樹型結構，其中連線到控制器的節點是RAP(Parent)。 第一個躍點另一端的直接節點是Child，第二個躍點後面的節點是該Parent的Neighbors。

圖1:兩跳網路



在圖1中，為了方便起見，提到了AP名稱。在下一個螢幕截圖中，**正在調查RAP(fb:10)**。此節點可以將（在實際部署中）室內網狀AP(**fa:60和b9:20)視為子**級，將**MAP ff:60視為鄰居**。

在交換器GUI介面中，依照路徑：**Wireless > All APs > Rap1 > Neighbor Info**。

確保正確建立和維護您的室內網狀網路的父子關係。

驗證互連

show Mesh是用於驗證網路中互連的資訊性命令。

您必須使用控制器CLI在每個節點(AP)處提供這些命令，並將結果以Word或文本檔案上傳到上傳站點。

```
(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.
```

在室內網狀網路中，選擇多跳鏈路並從RAP發出這些命令。將命令的結果上傳到上傳站點。

下一節中，已為圖1所示的兩跳室內網狀網路發出所有這些命令。

顯示室內網狀路徑

此命令將為您顯示特定路徑的MAC地址、節點的無線電角色、上行鏈路/下行鏈路(SNRUp、SNRDown)的dB中的訊雜比，以及dB中的鏈路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.
```

顯示室內網狀鄰居摘要

此命令將以數字為單位顯示MAC地址、父子關係和上行鏈路/下行鏈路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
```

此時，您應該能夠檢視網路節點之間的關係，並通過檢視每個鏈路的SNR值來驗證RF連線。

AP控制檯訪問安全

此功能增強了AP控制檯訪問的安全性。要使用此功能，AP需要使用控制檯電纜。

以下各項受支援：

- 用於將使用者ID/密碼組合推送到指定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.
```

- CLI命令將使用者名稱/密碼組合推送到註冊到控制器的所有
  AP:

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

通過這些命令，從控制器推送的使用者ID/密碼組合在AP上的重新載入中是持久的。如果從控制器中清除了AP，則沒有安全訪問模式。AP會生成一個成功登入的SNMP陷阱。AP還會連續三次在控制檯登入失敗時生成SNMP陷阱。

乙太網路橋接

出於安全原因，MAP上的乙太網埠預設處於禁用狀態。它只能通過在RAP和各自的MAP上配置乙太網橋接來啟用。

因此，必須為兩種情況啟用乙太網橋接：

- 當要將室內網狀節點用作網橋時。
- 當您希望使用其乙太網埠連線MAP上的任何乙太網裝置（例如PC/筆記型電腦、攝影機等）時
  。

路徑：**無線**>按一下任何AP > **Mesh**。

有一個CLI命令可用於配置執行橋接的節點之間的距離。嘗試在每一跳連線乙太網裝置（如影片監視器）以檢視效能。

Bridge Group Name增強

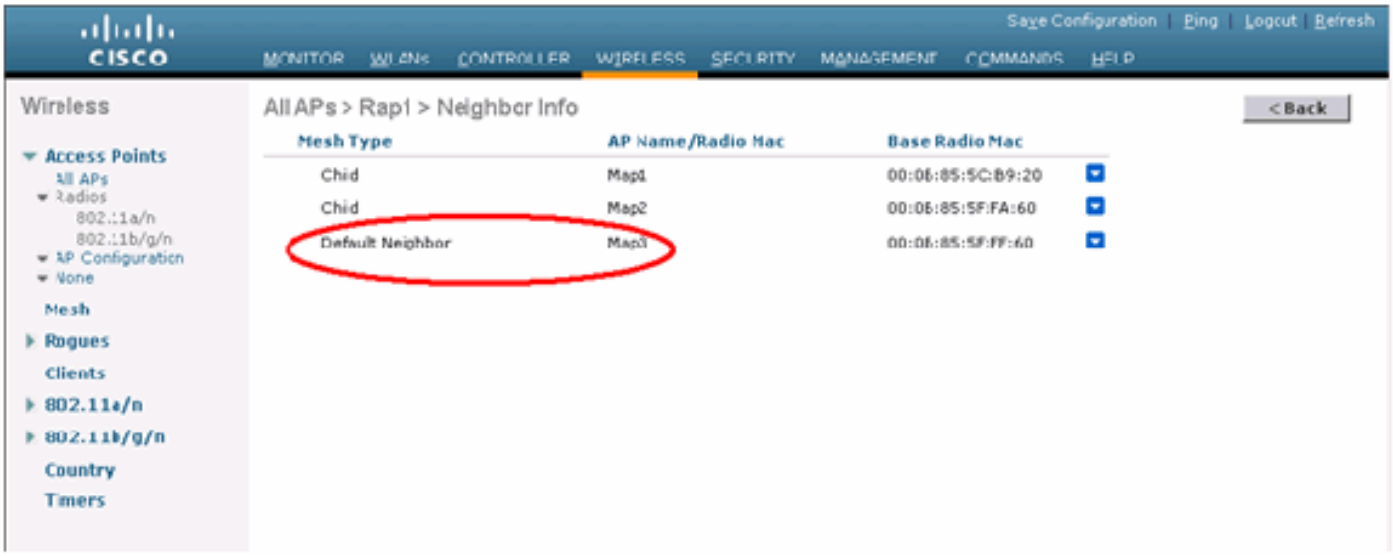
可能錯誤地為AP設定了「bridgegroupname」，而這是錯誤的。根據網路設計，此AP可能能夠找到並找到其正確的扇區/樹，也可能無法找到。如果無法到達相容的扇區，則它可能會被擱置。

為了恢復此類擱淺的AP，引入了「預設」橋組名稱的概念和3.2.xx.x代碼。其基本思想是，如果某個AP無法連線到其已配置的橋組名稱的任何其他AP，則嘗試使用「default」（單詞）作為橋組名稱進行連線。運行3.2.xx.x及更高版本軟體的所有節點都接受具有此橋組名稱的其他節點。

此功能也有助於向正在運行的網路中新增新節點或配置錯誤的節點。

如果您有一個正在運行的網路，請使用預配置的AP與不同的BGN並加入網路。在控制器中新增MAC地址後，您將在使用「預設」 BGN的控制器中看到此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
```



使用預設BGN的AP可以充當普通室內網狀AP，關聯客戶端並形成室內網狀父子關係。

當此AP使用預設BGN找到另一個具有正確BGN的父節點時，它將切換到該父節點。

日誌 — 消息、系統、AP和陷阱

消息日誌

啟用消息日誌的報告級別。在控制器CLI上，發出以下命令：

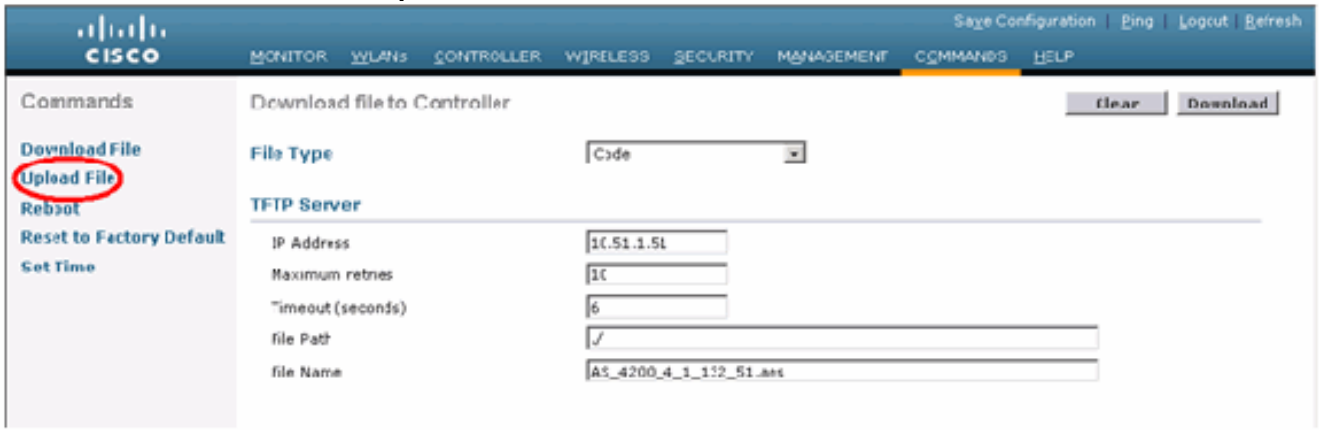
```
(Cisco Controller) >config msglog level ?

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
```

若要檢視訊息日誌，請從控制器CLI發出以下命令：

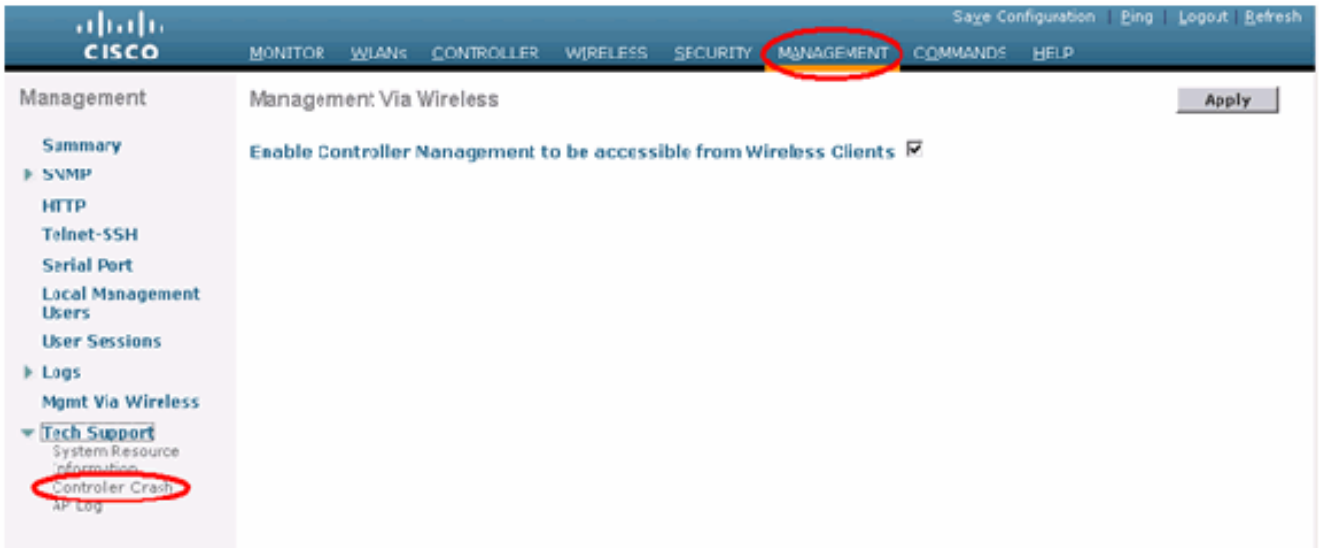
```
(Cisco Controller) >show msglog

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
```

若要上傳訊息日誌，請使用控制器GUI介面：

1. 按一下「Commands」>「Upload」。

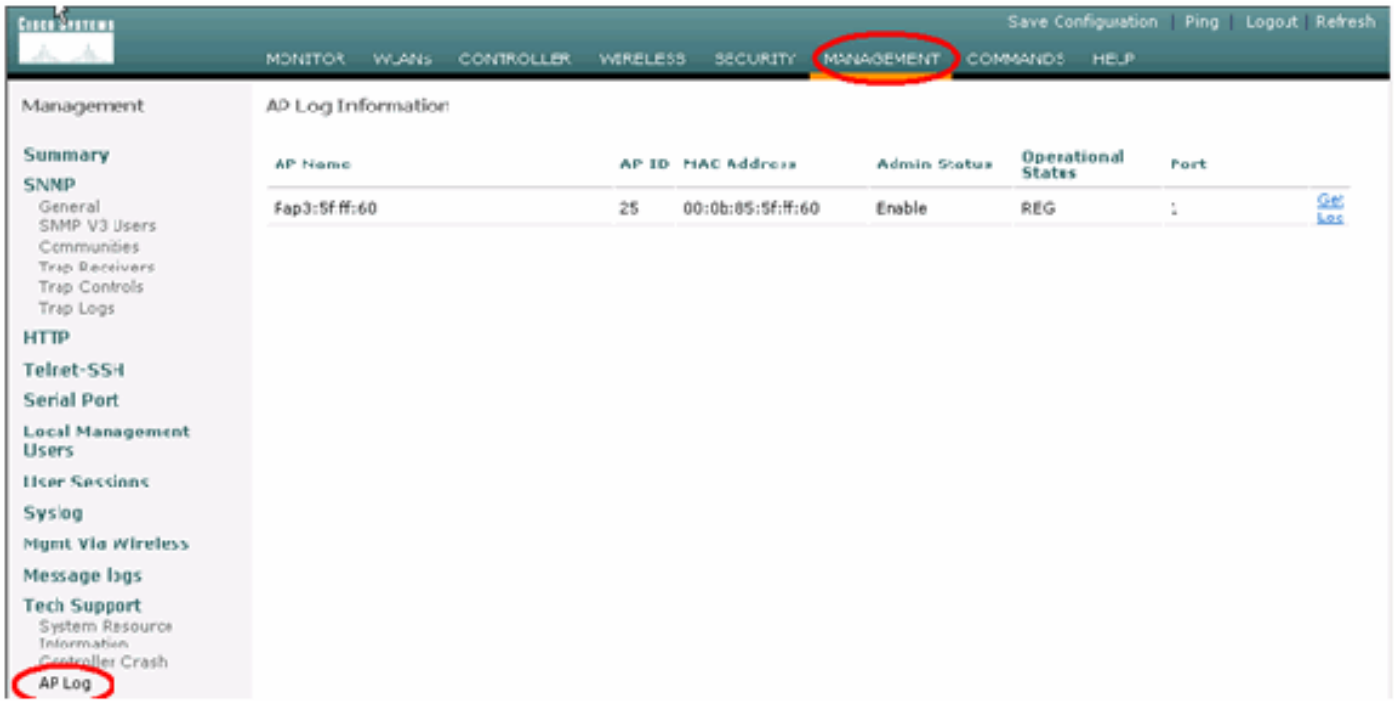


2. 輸入您的TFTP伺服器資訊。此頁面將為您提供各種上傳選項，您希望傳送以下檔案：消息日誌事件日誌陷阱日誌崩潰檔案（如果有）若要檢查崩潰檔案，請按一下Management > Controller Crash。



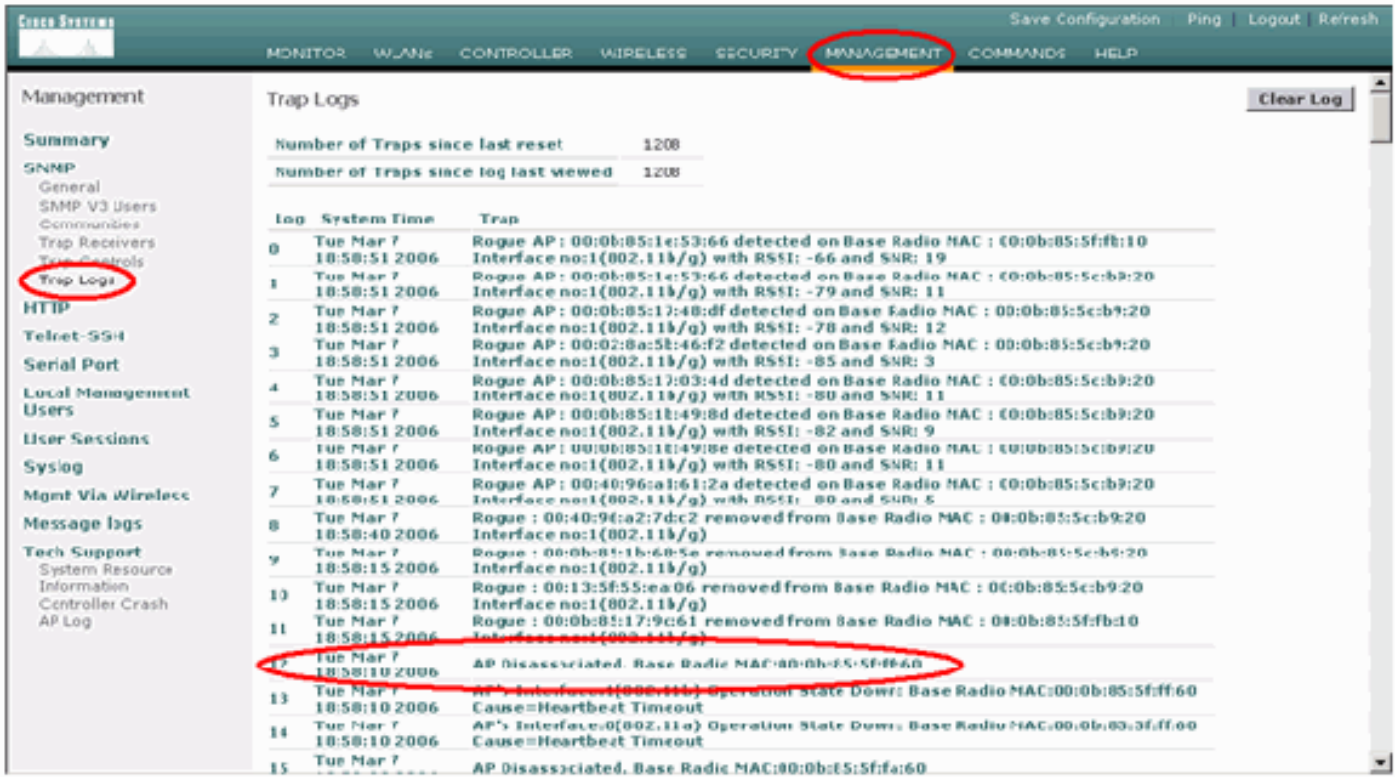
AP日誌

前往控制器上的此GUI頁面，檢查本地AP的AP日誌（如果有）：



陷阱日誌

前往控制器的此GUI頁面並檢查陷阱日誌：



效能

啟動收斂測試

Convergence是RAP/MAP與WLAN控制器建立穩定的LWAPP連線所用的時間，從它首次啟動時開始，如下所示：

收斂性測試	**收斂時間（分鐘：秒）**			
	RAP	MAP1	MAP2	對映3
映像升級	2:34	3:50	5:11	6:38
控制器重新啟動	0:38	0:57	1:12	1:32
室內網狀網路通電	2:44	3:57	5:04	6:09
RAP重新啟動	2:43	3:57	5:04	6:09
MAP重新加入		3:58	5:14	6:25
父級（同一通道）的MAP更改		0:38		

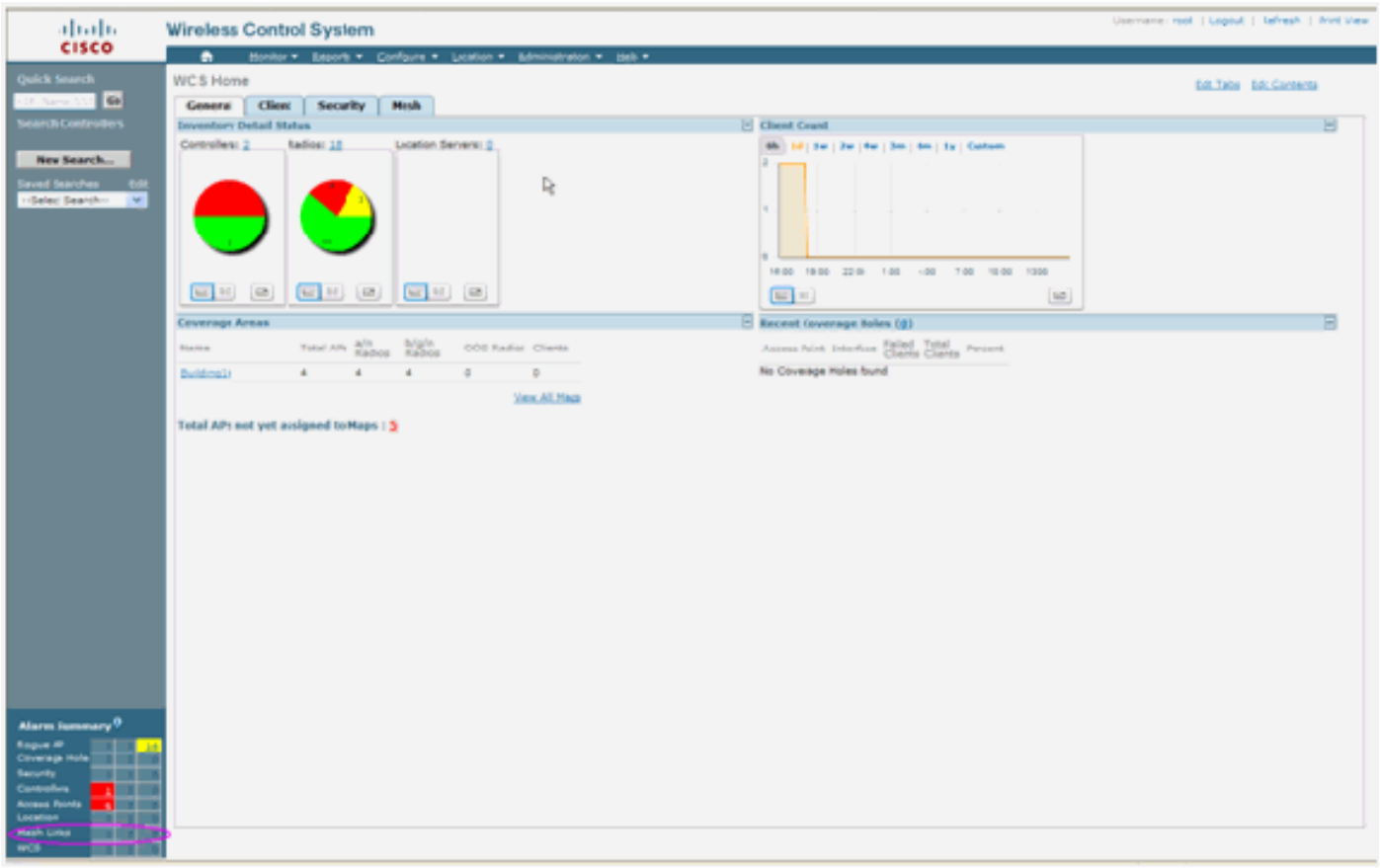
WCS

室內網狀警報

WCS將根據控制器中的陷阱生成與室內網狀網路相關的警報和事件：

- 鏈路訊雜比差
- 父項已更改
- 子項已移動
- MAP頻繁更改父項
- 控制檯埠事件
- MAC授權失敗
- 身份驗證失敗
- 子級排除的父級

按一下**網格連結**。它會顯示與室內網狀鏈路相關的所有警報。



以下警報適用於室內網狀鏈路：

- 鏈路訊雜比差 — 如果鏈路SNR低於12db，將生成此警報。使用者無法更改此閾值。如果在子級/父級的回程連結上偵測到較差的SNR，就會產生陷阱。陷阱將包含SNR值和MAC地址。警報嚴重性為嚴重。訊雜比(SNR)非常重要，因為高訊號強度不足以確保良好的接收機效能。輸入訊號必須比存在的任何雜訊或干擾都強。例如，如果存在強干擾或高雜訊電平，則可能具有高訊號強度且仍具有差無線效能。
- Parent changed — 當子項移動到另一個父項時生成此警報。當父節點丟失時，子節點將與另一個父節點加入，並且子節點會將包含舊父節點和新父節點的MAC地址的陷阱傳送到WCS。警報嚴重性：資訊。
- Child moved — 當WCS收到Child lost trap時生成此警報。當父AP檢測到其丟失了一個子節點且無法與該子節點通訊時，它將向WCS傳送Child lost trap。陷阱將包含子MAC地址。警報嚴重性：資訊。
- MAP父項頻繁更改 — 如果室內網狀AP頻繁更改其父項，則會生成此警報。當MAP parent-change-counter超過給定持續時間內的閾值時，它會向WCS傳送陷阱。陷阱將包含MAP更改的次數和持續時間。例如，如果在2分鐘內有5個更改，陷阱將被傳送。警報嚴重性：資訊。
- 子代排除的父代 — 當子代將父代列入黑名單時，將生成此警報。當子級在嘗試次數固定後無法在控制器上進行身份驗證時，子級可以將父級列入黑名單。子代會記住列入黑名單的父代，且當該子代加入網路時，它將傳送包含列入黑名單的父MAC地址和黑名單期限的陷阱。

除室內網狀鏈路外的警報：

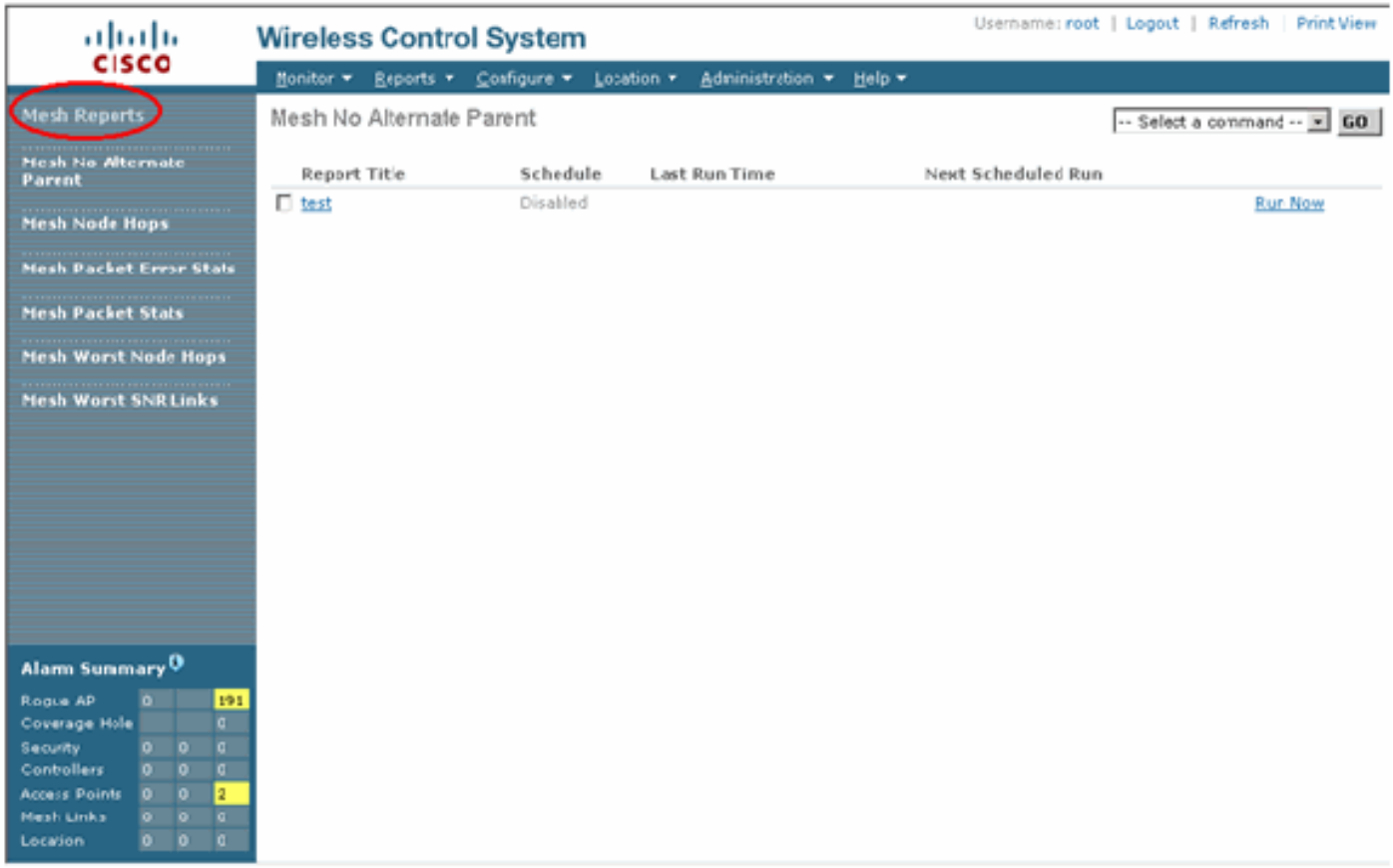
- 控制檯埠訪問 — 通過控制檯埠，客戶可以更改使用者名稱和密碼來恢復滯留的室外AP。但是，為防止任何授權使用者訪問AP，WCS需要在有人嘗試登入時發出警報。此警報用於提供保護，因為AP在室外易受物理攻擊。如果使用者成功登入到AP控制檯埠，或者連續三次失敗，將生成此警報。
- MAC Authorization Failure — 當AP嘗試加入室內網狀網路但無法進行身份驗證時，生成此警報，因為它不在MAC過濾器清單中。WCS將從控制器接收陷阱。陷阱將包含授權失敗的AP的

MAC地址。

網狀報告和統計資訊

我們將改進的報告和統計框架從4.1.185.0移到：

- 無備用路徑
- 網狀節點跳數
- 資料包錯誤統計資訊
- 資料包統計資訊
- 最差節點躍點
- 最差的SNR鏈路



無備用路徑

室內網狀AP通常有多個鄰居。當室內網狀AP丟失其父鏈路時，AP應該能夠找到備用父鏈路。在某些情況下，如果沒有顯示鄰居，則AP在失去其父項時將無法轉到任何其他父項。使用者必須知道哪些AP沒有備用父項。此報告列出除當前父項之外沒有任何其他鄰居的所有AP。

室內網狀節點跳數

此報告顯示遠離根AP(RAP)的跳數。 您可以根據以下條件建立報告：

- AP（按控制器）
- 按樓層劃分的接入點

封包錯誤率

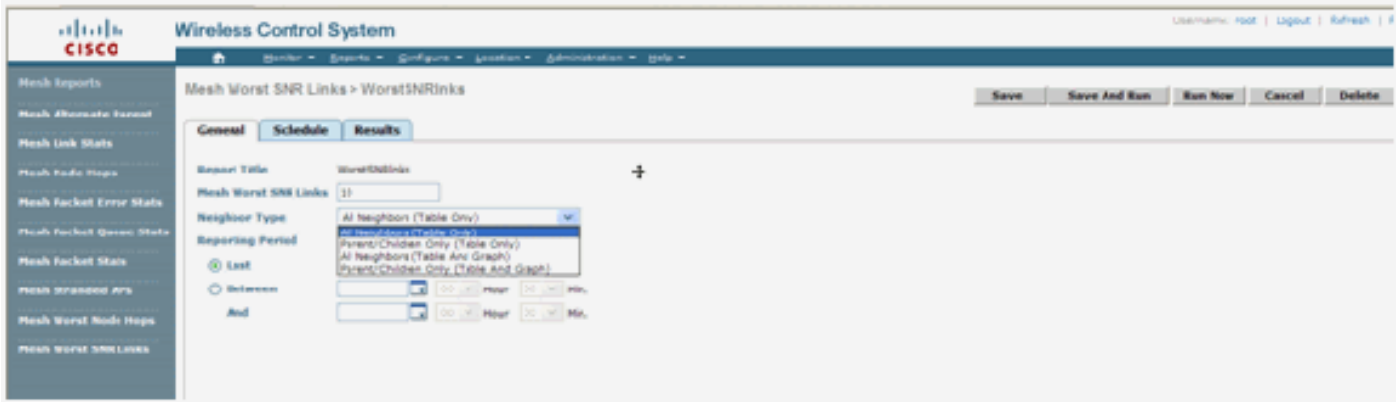
資料包錯誤可能是由干擾和丟包引起的。封包錯誤率計算基於已傳送的封包和成功傳送的封包。封包錯誤率是在回程連結上測量的，並為鄰居和父節點收集。AP定期向控制器傳送資料包資訊。一旦父交換機發生更改，AP就會將收集的資料包錯誤資訊傳送到控制器。預設情況下，WCS每10分鐘輪詢一次來自控制器的資料包錯誤資訊，並將其儲存在資料庫中長達7天。在WCS中，資料包錯誤率以圖形顯示。資料包錯誤圖基於儲存在資料庫中的歷史資料。

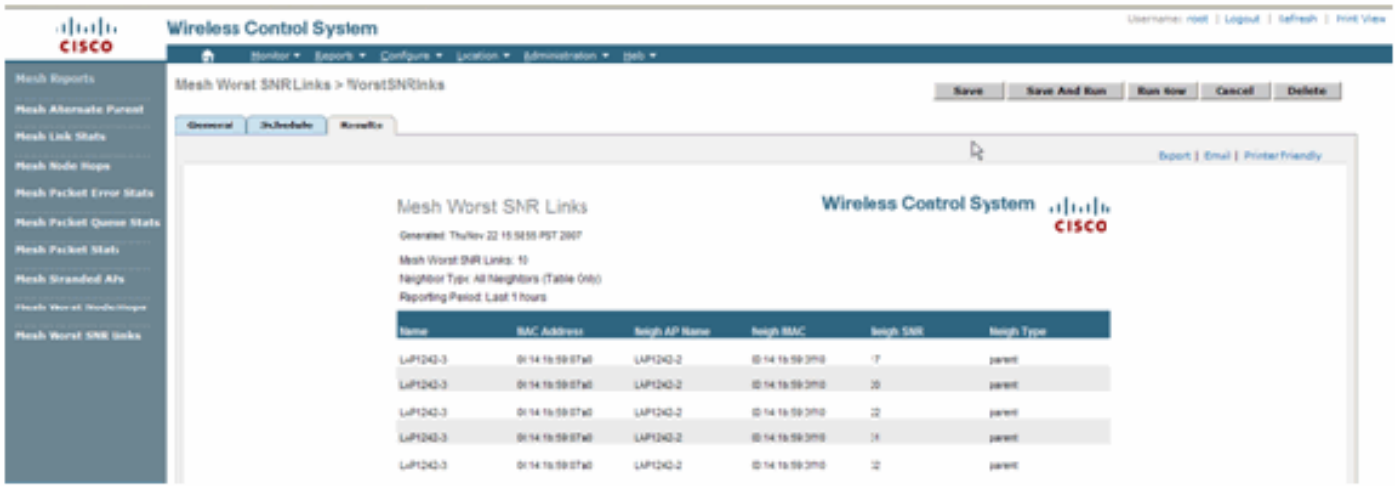
資料包統計資訊

此報告顯示成功傳輸的neighbor total傳輸資料包和Neighbor Total資料包的計數器值。您可以根據特定條件建立報告。

最差的SNR鏈路

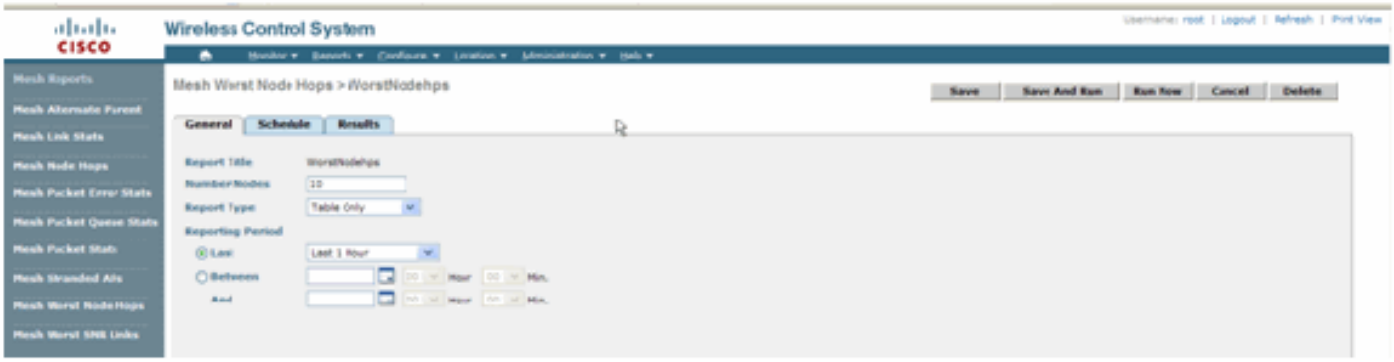
噪音問題可能發生在不同的時間，噪音可能會以不同的速度增加或持續不同的時間。下圖提供了為無線電a和b/g以及選擇性介面建立報告的功能。該報告預設列出10個最差的SNR鏈路。您可以選擇5到50個最糟糕的連結。可以為過去1小時、過去6小時、最後一天、過去2天以及最多7天生成報告。預設情況下，每10分鐘輪詢一次資料。資料在資料庫中最多儲存七天。鄰居型別選擇標準可以是「所有鄰居」，僅限父代/子代。



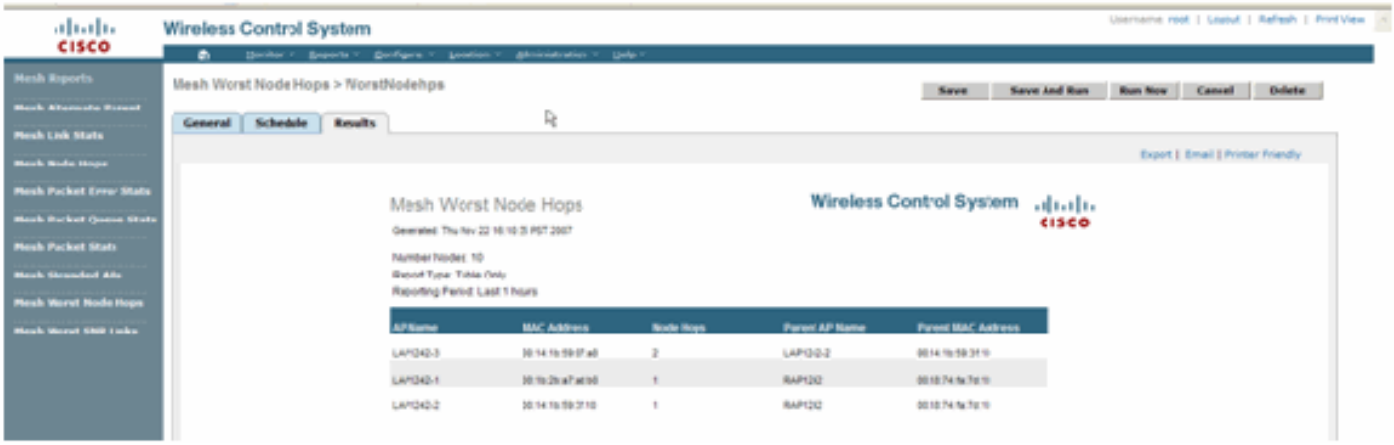


最差節點跳數

此報告預設列出10個最差跳AP。如果AP之間的跳數太多，鏈路可能非常薄弱。使用者可以隔離距離根AP有許多跳的AP並採取適當的措施。您可以選擇將此節點數**標準**從5更改為50。此圖中的**報告型別**篩選標準可以為「僅表」或「表和圖表」：



下圖顯示上次報告的結果：



安全統計

室內網狀安全統計資訊顯示在AP詳細資訊頁面的「橋接資訊」部分下。當子室內網狀節點與父室內網狀節點關聯或進行身份驗證時，會在室內網狀節點安全統計表中建立條目。當室內網狀節點與控制器解除關聯時，條目將被刪除。

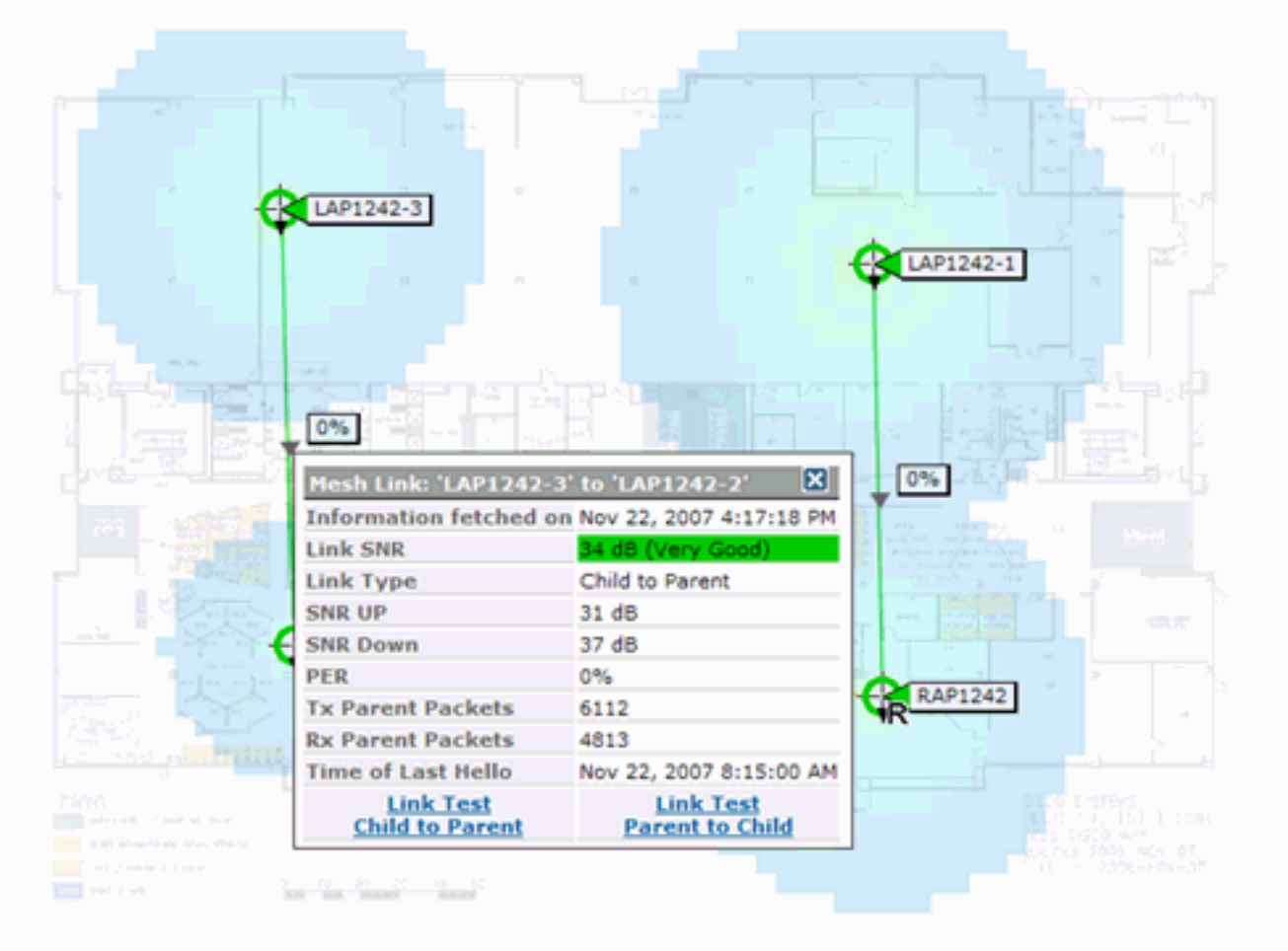
鏈路測試

WCS支援AP到AP鏈路測試。可以選擇任意兩個AP，並在兩者之間呼叫連結測試。

如果這些AP是RF鄰居，則鏈路測試可能會得到結果。結果顯示在對映本身的對話方塊中，沒有完整的頁面刷新。可以容易地處理該對話。

但是，如果這2個AP不是RF鄰居，則WCS不會嘗試在2個AP之間找出一條路徑，以便進行組合多鏈路測試。

當滑鼠移動到兩個節點之間的連結上的箭頭上時，出現以下視窗：



節點到節點鏈路測試

鏈路測試工具是驗證任意兩個AP之間的鏈路品質的按需工具。在WCS中，此功能將新增到AP詳細資訊頁面中。

在AP詳細資訊頁面的**Indoor Mesh Link**頁籤下（該頁籤旁邊列出了連結），有一個連結用於執行連結測試。

控制器CLI連結測試工具具有選用輸入引數：資料包大小、總鏈路測試資料包、測試持續時間和資料鏈路速率。連結測試具有這些可選引數的預設值。節點的MAC地址是唯一的強制輸入引數。

鏈路測試工具測試強度、傳送的資料包和節點間接收的資料包。鏈路測試連結顯示在AP詳細資訊報告中。按一下連結時，將顯示一個彈出螢幕，其中顯示了連結測試結果。鏈路測試僅適用於「父子」和鄰居之間。

Link Test輸出會生成Packets sent、Packets received、Error packets（由於不同原因而生成的儲存桶）、SNR、Noise Floor和RSSI。

Lnk測試至少在GUI上提供以下詳細資訊：

- 已傳送鏈路測試資料包
- 收到的鏈路測試資料包
- 訊號強度(dBm)
- 訊雜比

隨選AP鄰居鏈路

這是WCS對映中的新功能。您可以按一下網狀AP，此時將顯示一個包含詳細資訊資訊的彈出視窗。然後，可以按一下**檢視網狀鄰居**，這將獲取選定AP的鄰居資訊並顯示一個包含選定室內網狀點AP的所有鄰居的表。

「檢視網狀鄰居連結」顯示突出顯示的AP的所有鄰居。此快照顯示所有鄰居、鄰居的型別和SNR值。

Ping測試

Ping測試是一種按需工具，用於在控制器和AP之間執行ping。Ping測試工具在AP詳細資訊頁面和MAP中均可用。在AP詳細資訊頁面或從MAP AP資訊中按一下**Run Ping Test**連結，以啟動從控制器對當前AP的ping。

結論

企業網狀（即室內網狀）是思科無線覆蓋範圍的擴展，適用於有線乙太網無法提供連線的地方。通過企業網狀網路實現了無線網路的靈活性和可管理性。

有線AP提供的大多數功能由室內網狀拓撲提供。企業網狀也可與同一控制器上的有線AP共存。

相關資訊

- 技術支援與文件 - Cisco Systems