

ワイヤレス LAN コントローラのメッシュ ネットワークの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[Cisco Aironet 1510 シリーズ Lightweight 屋外メッシュ AP](#)

[Roof-top Access Point \(RAP; ルーフトップ アクセス ポイント \)](#)

[Pole-top Access Point \(PAP; ポールトップ アクセス ポイント \)](#)

[メッシュ ネットワークでサポートされない機能](#)

[アクセス ポイントのスタートアップ シーケンス](#)

[設定](#)

[ゼロタッチ設定の有効化 \(デフォルトで有効 \)](#)

[AP 認証リストへの MIC の追加](#)

[AP 用のブリッジング パラメータの設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、メッシュ ネットワーク ソリューションを使用して、ポイントツーポイントのブリッジド リンクを確立する方法を示す、基本的な設定例を説明します。この例では、2 つの Lightweight Access Point (LAP; Lightweight アクセス ポイント) が使用されています。1 つの LAP は Roof-top Access Point (RAP; ルーフトップ アクセス ポイント) として動作し、他の LAP は Pole-top Access Point (PAP; ポールトップ アクセス ポイント) として動作します。これらは 2 つとも Cisco Wireless LAN (WLAN; ワイヤレス LAN) Controller (WLC; ワイヤレス LAN コントローラ) に接続されています。RAP は Cisco Catalyst スイッチを介して WLC に接続されています。

WLCリリースのリリース5.2以降のWireless LANコントローラの[メッシュ ネットワークの設定例を5.2以降のバージョンを参照してください](#)

前提条件

- WLC は基本動作用に設定されています。

- WLC はレイヤ 3 モードで設定されています。
- WLC 用のスイッチが設定されています。

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- LAP および Cisco WLC の設定に関する基礎知識
- Lightweight AP Protocol (LWAPP) に関する基本的な知識。
- 外部 DHCP サーバおよび Domain Name Server (DNS; ドメイン ネーム サーバ) のどちらかまたは両方の設定に関する知識
- Cisco スwitch の設定に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ファームウェア 3.2.150.6 が稼働する Cisco 4402 シリーズ WLC
- 2 基の Cisco Aironet 1510 シリーズ LAP
- Cisco レイヤ 2 スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景説明

Cisco Aironet 1510 シリーズ Lightweight 屋外メッシュ AP

Cisco Aironet 1510 シリーズ Lightweight 屋外メッシュ AP は、ワイヤレス クライアントのアクセスとポイントツーポイントのブリッジング、ポイントツーマルチポイントのブリッジング、およびポイントツーマルチポイントのメッシュ型ワイヤレス接続用に設計されたワイヤレス デバイスです。屋外アクセス ポイントは、壁または突出部分、ルーフトップ ポール、または街灯のポールに設置可能な独立型の装置です。

AP1510 はコントローラとともに動作して、中央集中型でスケーラブルな管理、高度なセキュリティ、および、モビリティを実現します。AP1510 は設定不要で配置できる設計になっているので、メッシュ型ネットワークに簡単かつセキュアに加入でき、コントローラの GUI または CLI を使用してネットワークの管理と監視が行えます。

AP1510は二つの同時実行の無線を備えた:他のAP1510sへのアクセスとデータ バックホールに使用する5 GHz無線使用する2.4 GHz無線。ワイヤレス LAN のクライアントトラフィックは、コントローラのイーサネット接続に到達するまでは AP のバックホール無線を使用して転送、つまり、他の AP1510 を通して中継されます。

Roof-top Access Point (RAP; ルーフトップ アクセス ポイント)

RAP は、Cisco WLC に有線接続されています。RAP はバックホール ワイヤレス インターフェイスを使用して、隣接する PAP と通信します。RAP は、ブリッジング ネットワークやメッシュ ネットワークの親ノードであり、ブリッジ ネットワークやメッシュ ネットワークを有線ネットワークに接続する役割を果たしています。そのため、ブリッジド ネットワークやメッシュ ネットワークのセグメントに存在できる RAP は 1 つだけになります。

注：LAN-to-LANブリッジングにメッシュネットワークソリューションを使用する場合は、RAPをCisco WLCに直接接続しないでください。Cisco WLC は LWAPP が有効なポートからのイーサネットトラフィックを転送しないので、Cisco WLC と RAP の間にスイッチルータが必要になります。RAP は、レイヤ 2 またはレイヤ 3 の LWAPP モードで動作可能です。

Pole-top Access Point (PAP; ポールトップ アクセス ポイント)

PAP は、Cisco WLC に有線接続されていません。PAP は完全にワイヤレスにすることが可能で、他の PAP や RAP と通信するクライアントをサポートすることも、周辺デバイスや有線ネットワークへの接続に使用することもできます。デフォルトでは、セキュリティ上の理由によりイーサネット ポートが無効になっていますが、PAP 用には有効にしてください。

注：Cisco Aironet 1030リモートエッジLAPはシングルホップ展開をサポートし、Cisco Aironet 1500シリーズLightweight屋外APはシングルホップ展開とマルチホップ展開の両方をサポートします。そのため、Cisco Aironet 1500 シリーズ Lightweight 屋外 AP は、Cisco WLC から 1 つ以上のホップがある場合のルーフトップ AP や PAP として使用できます。

メッシュ ネットワークでサポートされない機能

次のコントローラの機能は、メッシュ ネットワークではサポートされていません。

- 複数国サポート
- ロード ベースの CAC (メッシュ ネットワークは帯域幅ベース、またはスタティックの CAC のみサポートしています)
- ハイ アベイラビリティ (高速ハートビートとプライマリ ディスカバリ結合タイマーに参加します)
- EAP-FASTv1 および 802.1X 認証
- EAP-FASTv1 および 802.1X 認証
- Locally Significant Certificate; ローカルで有効な証明書
- ロケーション ベース サービス

アクセス ポイントのスタートアップ シーケンス

次のリストは、RAP と PAP のスタートアップ時に起きる事柄を説明しています。

- すべてのトラフィックは、LAN に送信される前に RAP と Cisco WLC を通過します。
- RAP が起動されると、PAP は自動的に RAP に接続されます。
- 接続されたリンクでは、共有秘密を使用して、リンクの Advanced Encryption Standard (AES; 高度暗号化規格) を実現するために使用するキーが生成されます。
- リモート PAP が RAP に接続されると、メッシュの AP がデータトラフィックを渡せるようになります。

- ユーザは、シスコのコマンドライン インターフェイス (CLI)、コントローラのシスコ Web ユーザ インターフェイス、または Cisco Wireless Control System (Cisco WCS) を使用して、共有秘密を変更したりメッシュ AP を設定したりできます。共有秘密は変更することをお勧めします。



設定

WLC と AP をポイントツーポイントのブリッジング用に設定するには、次のステップを実行します。

1. [WLC のゼロタッチ設定を有効にします。](#)
2. [AP 認証リストに MIC を追加します。](#)
3. [AP 用のブリッジング パラメータを設定します。](#)
4. [設定を確認します。](#)

ゼロタッチ設定の有効化 (デフォルトで有効)

GUI での設定

Enable Zero Touch Configuration をオンにすると、AP が WLC に登録されたときにコントローラから共有秘密キーを AP が入手できるようになります。このチェックボックスをオフにすると、コントローラからは共有秘密キーが提供されず、AP はデフォルトの事前共有キーを使用してセキュアな通信を行います。デフォルトでは有効 (オン) になっています。WLC の GUI から次の手順を実行します。

注 : WLCバージョン4.1以降では、ゼロタッチ設定のプロビジョニングはありません。

1. >ブリッジング[Wireless]を選択し、ゼロタッチで、[Enable]をクリックします。
2. Key Format を選択します。
3. Bridging Shared Secret Key にブリッジングの共有秘密キーを入力します。
4. Confirm Shared Secret Key にブリッジングの共有秘密キーをもう一度入力します。

Wireless

Access Points
All APs
802.11a Radios
802.11b/g Radios
Third Party APs

Bridging

Rogues
Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues

Clients

Global RF
802.11a Network
802.11b/g Network
802.11h

Country

Timers

Bridging

Zero Touch Configuration

Enable Zero Touch Configuration

Key Format

Bridging Shared Secret Key

Confirm Shared Secret Key

CLI での設定

CLI から次の手順を実行します。

1. `config network zero-config enable` コマンドを発行して、ゼロタッチ設定を有効にします。
(Cisco Controller) `>config network zero-config enable`
2. ブリッジの共有秘密キーを追加するには、`config networkブリッジング共有秘密を<string>`のコマンドを発行します。
(Cisco Controller) `>config network bridging-shared-secret Cisco`

[AP 認証リストへの MIC の追加](#)

次の手順として、WLC の認証リストに AP を追加します。これを行うには、> APポリシーの [Security]を選択し、APのMACアドレス、およびAPの認証リストに[Add]をクリックして入力します。

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

AP Policies

Policy Configuration

Authorize APs against AAA Enabled

Accept Self Signed Certificate Enabled

Apply

Add AP to Authorization List

MAC Address

Certificate Type

Add

AP Authorization List Items 0 to 20 of 0

MAC Address	Certificate Type	SHA1 Key Hash
-------------	------------------	---------------

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

AP Policies

Policy Configuration

Authorize APs against AAA Enabled

Accept Self Signed Certificate Enabled

Add AP to Authorization List

MAC Address

Certificate Type

AP Authorization List Items 1 to 2 of 2

MAC Address	Certificate Type	SHA1 Key Hash
00:0b:85:5e:40:00	MIC	
00:0b:85:5e:5a:80	MIC	

この例では、両方の AP (RAP と PAP) が、コントローラの AP 認証リストに追加されています。

CLI での設定

組織の認証リストを許可リストにMICを追加するには、[Add aマイク<APのmac>]のコマンドを発行します。

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80
```

コンフィギュレーション

このドキュメントでは、次の設定を使用しています。

Cisco WLC 4402

```
(Cisco Controller) >show run-config
```

```
Press Enter to continue...
```

System Inventory

```
Switch Description..... Cisco  
Controller  
Machine Model.....  
WLC4402-12  
Serial Number.....  
FLS0943H005  
Burned-in MAC Address.....  
00:0B:85:40:CF:A0  
Crypto Accelerator 1..... Absent  
Crypto Accelerator 2..... Absent  
Power Supply 1..... Absent  
Power Supply 2.....  
Present, OK
```

```
Press Enter to continue Or <Ctl Z> to abort
```

System Information

```
Manufacturer's Name..... Cisco  
Systems, Inc  
Product Name..... Cisco  
Controller  
Product Version.....  
3.2.150.6  
RTOS Version.....  
3.2.150.6  
Bootloader Version.....  
3.2.150.6  
Build Type..... DATA +  
WPS  
  
System Name.....  
lab120wlc4402ip100  
System Location.....  
System Contact.....  
System ObjectID.....  
1.3.6.1.4.1.14179.1.1.4.3  
IP Address.....  
192.168.120.100  
System Up Time..... 0 days  
1 hrs 4 mins 6 secs  
  
Configured Country..... United  
States  
Operating Environment.....  
Commercial (0 to 40 C)  
Internal Temp Alarm Limits..... 0 to  
65 C  
Internal Temperature..... +42 C
```

State of 802.11b Network.....
Disabled
State of 802.11a Network.....
Disabled
Number of WLANs..... 1
3rd Party Access Point Support.....
Disabled
Number of Active Clients..... 0

Press Enter to continue Or <Ctl Z> to abort

Switch Configuration

802.3x Flow Control Mode.....
Disable
Current LWAPP Transport Mode..... Layer
3
LWAPP Transport Mode after next switch reboot.... Layer
3
FIPS prerequisite features.....
Disabled

Press Enter to continue Or <Ctl Z> to abort

Network Information

RF-Network Name..... airespacerf
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable
Mode: Ucast
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Enable
Bridge AP Zero Config..... Enable
Bridge Shared Secret.....
youshouldsetme
Allow Old Bridging Aps To Authenticate..... Disable
Over The Air Provisioning of AP's..... Disable
Mobile Peer to Peer Blocking..... Disable
Apple Talk Disable
AP Fallback Enable
Web Auth Redirect Ports 80
Fast SSID Change Disabled

Press Enter to continue Or <Ctl Z> to abort

Port Summary

	STP	Admin	Physical	Physical	Link
Link	Mcast				
Pr	Type	Stat	Mode	Status	Status
Trap	Appliance	POE			
1	Normal	Forw	Enable	Auto	1000 Full Up
	Enable	Enable	N/A		
2	Normal	Forw	Enable	Auto	1000 Full Up
	Enable	Enable	N/A		

Mobility Configuration

Mobility Protocol Port..... 16666
Mobility Security Mode.....


```

Disabled
Default Mobility Domain.....
airespacerf
Mobility Group members configured..... 3

Switches configured in the Mobility Group
MAC Address          IP Address          Group Name
00:0b:85:33:a8:40    192.168.5.70       <local>
00:0b:85:40:cf:a0    192.168.120.100    <local>
00:0b:85:43:8c:80    192.168.5.40       airespacerf

Interface Configuration
Interface Name..... ap-
manager
IP Address.....
192.168.120.101
IP Netmask.....
255.255.255.0
IP Gateway.....
192.168.120.1
VLAN.....
untagged
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port.....
Unconfigured
Primary DHCP Server.....
192.168.1.20
Secondary DHCP Server.....
Unconfigured
ACL.....
Unconfigured
AP Manager..... Yes

Interface Name.....
management
MAC Address.....
00:0b:85:40:cf:a0
IP Address.....
192.168.120.100
IP Netmask.....
255.255.255.0
IP Gateway.....
192.168.120.1
VLAN.....
untagged
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port.....
Unconfigured
Primary DHCP Server.....
192.168.1.20
Secondary DHCP Server.....
Unconfigured
ACL.....
Unconfigured
AP Manager..... No

Interface Name.....
service-port
MAC Address.....
00:0b:85:40:cf:a1
IP Address.....
192.168.250.100

```

```

IP Netmask.....
255.255.255.0
DHCP Protocol.....
Disabled
AP Manager..... No

Interface Name.....
virtual
IP Address.....
1.1.1.1
Virtual DNS Host Name.....
Disabled
AP Manager..... No

WLAN Configuration

WLAN Identifier..... 1
Network Name (SSID).....
lab120wlc4402ip100
Status.....
Enabled
MAC Filtering.....
Enabled
Broadcast SSID.....
Enabled
AAA Policy Override.....
Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60
seconds
Session Timeout..... 1800
seconds
Interface.....
management
WLAN ACL.....
unconfigured
DHCP Server.....
Default
Quality of Service..... Silver
(best effort)
WMM.....
Disabled
802.11e.....
Disabled
Dot11-Phone Mode (7920).....
Disabled
Wired Protocol..... None
IPv6 Support.....
Disabled
Radio Policy..... All
Radius Servers
  Authentication.....
192.168.1.20 1812
Security

  802.11 Authentication:..... Open
System
  Static WEP Keys.....
Enabled
    Key Index:.....
1
    Encryption:.....
104-bit WEP
  802.1X.....

```

```

Disabled
  Wi-Fi Protected Access (WPA1).....
Disabled
  Wi-Fi Protected Access v2 (WPA2).....
Disabled
  IP Security.....
Disabled
  IP Security Passthru.....
Disabled
  L2TP.....
Disabled
  Web Based Authentication.....
Disabled
  Web-Passthrough.....
Disabled
  Auto Anchor.....
Disabled
  Cranite Passthru.....
Disabled
  Fortress Passthru.....
Disabled

RADIUS Configuration
Vendor Id Backward Compatibility.....
Disabled
Credentials Caching.....
Disabled
Call Station Id Type..... IP
Address
Administrative Authentication via RADIUS.....
Enabled
Keywrap.....
Disabled

Load Balancing Info
Aggressive Load Balancing.....
Enabled
Aggressive Load Balancing Window..... 0
clients

Signature Policy
  Signature Processing.....
Enabled

Spanning Tree Switch Configuration

STP Specification..... IEEE 802.1D
STP Base MAC Address.....
00:0B:85:40:CF:A0
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15

Spanning Tree Port Configuration

STP Port ID..... 8001
STP Port State..... Forwarding
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 4
STP Port Path Cost Mode..... Auto

```

STP Port ID.....	8002
STP Port State.....	Forwarding
STP Port Administrative Mode.....	802.1D
STP Port Priority.....	128
STP Port Path Cost.....	4
STP Port Path Cost Mode.....	Auto

AP用のブリッジングパラメータの設定

このセクションでは、メッシュネットワーク内のAPの役割の設定方法および関連するブリッジングパラメータについて説明します。これらのパラメータは、GUIかCLIのどちらかを使用して設定できます。

1. [Wireless] をクリックして、次に [Access Points] の下の [All APs] をクリックします。[All APs] ページが表示されます。
2. ご使用の AP1510 の [Detail] リンクをクリックして、[All APs] > [Details] ページにアクセスします。

このページでは、AP1510などのブリッジ機能を持つAPに対して、[General]の[AP Mode]が自動的に[Bridge]に設定されます。このページの[Bridging Information]にもこの情報が表示されます。[Bridging Information] で、次のオプションのいずれかを選択して、メッシュネットワーク内のこのAPの役割を指定します。

- **MeshAP:** AP1510がコントローラにワイヤレス接続されている場合は、このオプションを選択します。
- **RootAP:** AP1510がコントローラに有線接続されている場合は、このオプションを選択します。

Bridging Information

AP Role	MeshAP ▼
Bridge Type	Outdoor
Bridge Group Name	<input type="text"/>
Ethernet Bridging	<input type="checkbox"/>
Backhaul Interface	802.11a
Bridge Data Rate (Mbps)	18 ▼

確認

ここでは、設定が正常に機能しているかどうかを確認します。

APがWLCに登録されると、WLCのGUIの上部にあるWirelessタブでAPを表示できるようになります。

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
lab120br1510ip152	8	00:0b:85:5e:5a:80	Enable	REG	1	Detail Bridging Information
lab120br1510ip150	10	00:0b:85:5e:40:00	Enable	REG	1	Detail Bridging Information

CLI では、show ap summary コマンドを使用して、AP が WLC に登録されたことを次のように確認できます。

(Cisco Controller) > **show ap summary**

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
lab120br1510ip152	2	OAP1500	00:0b:85:5e:5a:80	default_location	1
lab120br1510ip150	2	OAP1500	00:0b:85:5e:40:00	default_location	1

(Cisco Controller) >

GUI の Bridging Details をクリックして、AP の役割を確認します。

Bridging Details		Bridging Links	
AP Role	RAP	Parent	
Bridge Group Name		Child	lab120br1510ip150 : 00:0b:85:5e:
Backhaul Interface	802.11a		
Switch Physical Port	1		
Routing State	Maintenance		
Malformed Neighbor Packets	0		
Poor Neighbor SNR reporting	0		
Blacklisted Packets	0		
Insufficient Memory reporting	0		
Rx Neighbor Requests	37		
Rx Neighbor Responses	0		
Tx Neighbor Requests	0		
Tx Neighbor Responses	37		
Parent Changes count	0		
Neighbor Timeouts count	0		
Node Hops	0		

WLC CLI で show mesh path <Cisco AP> コマンドおよび show mesh neigh <Cisco AP> コマンドを使用して、AP が WLC に登録されていることを確認できます。

```
(Cisco Controller) >show mesh path lab120br1510ip152
00:0B:85:5E:5A:80 is RAP
```

```
(Cisco Controller) >show mesh neigh lab120br1510ip152
```

```
AP MAC : 00:0B:85:5E:40:00
```

```
FLAGS : 160 CHILD
```

```
worstDv 255, Ant 0, channel 0, biters 0, ppiters 10
```

```
Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0
```

```
adjustedEase 0, unadjustedEase 0
```

```
txParent 0, rxParent 0
```

```
poorSnr 0
```

```
lastUpdate 1150103792 (Mon Jun 12 09:16:32 2006)
```

```
parentChange 0
```

```
Per antenna smoothed snr values: 0 0 0 0
```

```
Vector through 00:0B:85:5E:40:00
```

```
(Cisco Controller) >
```

トラブルシュート

APWLC 次の確認を行ってください。

1. アクセスポイントの MAC アドレスが WLC の MAC フィルタ リストに追加されていることを確認します。これは、`セキユリテイ> Mac Filtering]`で確認できます。
2. RAPとMAP間の共有秘密情報を確認します。キーが一致しなかった場合は、WLCで次のメッセージを表示できます。`LWAPPAUTH_STRING_PAYLOADAP 00:0b:85:68:c1:d0` 注：バージョンにより、**ゼロ タッチの設定オプション**を使用して常にします (可能な場合)。これは自動的にメッシュAPのキーを設定し、誤設定を回避できます。
3. RAPは無線インターフェイスのプロードキャスト メッセージを転送しません。従ってマップがIPアドレスをRAPによって転送されるよう、ユニキャストではIPアドレスを送信するようにDHCPサーバを設定します。そうマッピングのスタティックIPを使用します。
4. ブリッジグループ名をデフォルト値のままにするか、またはブリッジグループ名がマッピングおよび対応するRAPと同じように設定されていることを確認します。

これらは、メッシュ アクセス ポイントは、特定の問題です。WLCとアクセス ポイント間で共通の接続の問題について[トラブルシューティングするワイヤレスLANコントローラに参加しない Lightweightアクセス ポイントを参照してください。](#)

トラブルシューティングのためのコマンド

注：`debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

次のデバッグ コマンドを使用して、WLC のトラブルシューティングを行えます。

- [debug pem state enable](#) : アクセス ポリシー マネージャのデバッグ オプションの設定に使用

します。

- [debug pem events enable](#) : アクセス ポリシー マネージャのデバッグ オプションの設定に使用します。
- [debug dhcp message enable](#) : DHCP サーバとの間で相互に交換された DHCP メッセージのデバッグ情報が表示されます。
- [debug dhcp packet enable](#) : DHCP サーバとの間で相互に送信された DHCP パケットの詳細なデバッグ情報が表示されます。

次の debug コマンドもトラブルシューティングに使用できます。

- [debug lwapp errors enable](#) : LWAPP エラーのデバッグ情報が表示されます。
- [debug pm pki enable](#) : AP と WLC の間で渡された証明書メッセージのデバッグ情報が表示されます。

次の debug lwapp events enable WLC コマンドの出力は、LAP が WLC に登録されたことを示しています。

```
(Cisco Controller) >debug lwapp events enable
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 Received LWAPP JOIN REQUEST  
from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1'
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce  
00:0B:85:40:CF:A0 rxNonce 00:0B:85:5E:40:00
```

```
Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from  
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully added NPU Entry for  
AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101, Switch Port: 12223,  
intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop  
MAC: 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of  
LWAPP Join-Reply to AP 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP  
00:0b:85:5e:40:00 slot 0
```

```
Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP  
00:0b:85:5e:40:00 slot 1
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE REQUEST  
from AP 00:0b:85:5e:40:00 to 00:0b:85:40:cf:a3
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00  
-- static 1, 192.168.120.150/255.255.255.0, gtw 192.168.120.1
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring  
-A regDfromCb -A
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring  
-A regDfromCb -A
```

```
Mon Jun 12 09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret  
airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to  
AP 00:0b:85:5e:40:00
```

```
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP  
Config-Message to AP 00:0b:85:5e:40:00
```

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00 associated.
Last AP failure was due to Link Failure, reason: STATISTICS_INFO_RES

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext:
Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for
AP 00:0b:85:5e:40:00 slot 0!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext:
Down LWAPP event for AP 00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP
00:0b:85:5e:40:00 slot 1!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

関連情報

- [Cisco メッシュ ネットワーキング ソリューション導入ガイド](#)
- [クイックスタート ガイドCisco Aironet 1500 シリーズ Lightweight 屋外メッシュ アクセス ポイント](#)
- [Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0](#)
- [ワイヤレスに関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)