トラブルシューティング

この章では、トラブルシューティング情報について説明します。内容は次のとおりです。

インストールと接続

ステップ 1 RAP にするメッシュ アクセス ポイントをコントローラに接続します。

ステップ 2 目的の場所に無線（MAP）を配置します。

ステップ 3 コントローラ CLI で、**show mesh ap summary** コマンドを入力して、コントローラ上のすべての MAP と RAP を表示します。

図 *1*：*[Mesh AP Summary]* ページの表示

```
(Cisco Controller) >show mesh ap summary

AP Name                AP Model             BVI MAC            CERT MAC       Hop  Bridge Group Name  Enhanced Feature Set
-----------------  -------------------  -----------------  -----------------  ---  -----------------  --------------------
1532MAP2-DaisyChained  AIR-CAP1532E-A-K9    4c:4e:35:46:f2:72  4c:4e:35:46:f2:72  0    default            N/A
1532RAP1             AIR-CAP1532E-A-K9    4c:4e:35:46:f2:64  4c:4e:35:46:f2:64  0    default            N/A
1532MAP1             AIR-CAP1532E-A-K9    4c:4e:35:46:f1:4e  4c:4e:35:46:f1:4e  1    default            N/A
1524PSRAP1           AIR-LAP1524PS-A-K9   00:22:be:41:23:00  00:22:be:41:23:00  0    MESHDEMO1          N/A
1522MAP2             AIR-LAP1522AG-A-K9   00:22:be:42:fe:00  00:22:be:42:fe:00  1    MESHDEMO1          N/A

Number of Mesh APs.............................. 3
Number of RAPs.................................. 2
Number of MAPs.................................. 1
Number of Flex+Bridge APs....................... 2
Number of Flex+Bridge RAPs...................... 1
Number of Flex+Bridge MAPs...................... 1
```

ステップ 4 コントローラ GUI で、[Wireless] をクリックして、メッシュ アクセス ポイント（RAP と MAP）の概要を表示します。

図 *2*：*[All APs Summary]* ページ

All APs

Search by AP MAC Search

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certific Type
iMeshRap1	00:19:30:76:32:72	0 d, 22 h 24 m 25 s	Enable	REG	Local	MIC
HJRAP1	00:1d:71:0d:e1:00	0 d, 22 h 12 m 37 s	Enable	REG	Bridge	MIC
HJMAP3	00:1d:71:0d:d5:00	0 d, 22 h 05 m 04 s	Enable	REG	Bridge	MIC
HJMAP1	00:1d:71:0c:f4:00	0 d, 22 h 04 m 48 s	Enable	REG	Bridge	MIC
HJMAP2	00:1d:71:0c:f0:00	0 d, 22 h 04 m 53 s	Enable	REG	Bridge	MIC
HPRAP1	00:1e:14:48:43:00	0 d, 05 h 35 m 24 s	Enable	REG	Bridge	MIC
HPMAP1	00:1b:d4:a7:78:00	0 d, 22 h 04 m 25 s	Enable	REG	Bridge	MIC

273952

ステップ 5 [AP Name] をクリックして詳細ページを表示し、[Interfaces] タブを選択して、アクティブな無線インターフェイスを表示します。
使用中の無線スロット、無線タイプ、使用中のサブバンド、動作状態（UP または DOWN）がまとめて表示されます。

- すべての AP は 2 つの無線スロット（スロット 0 - 2.4 GHz とスロット 1 – 5 GHz）をサポートしています。

  同じメッシュ ネットワークに複数のコントローラを接続している場合、すべてのメッシュ アクセス ポイントに対するグローバル設定を使用してプライマリ コントローラの名前を指定するか、各ノードでプライマリ コントローラを指定する必要があります。指定しないと、負荷が最小のコントローラが優先されます。メッシュ アクセス ポイントがコントローラに以前接続されていた場合、メッシュ アクセス ポイントはコントローラの名前をすでに認識しています。

  コントローラ名の設定後、メッシュ アクセス ポイントがリブートします。

ステップ 6 [Wireless] > [AP Name] をクリックして、AP 詳細ページでメッシュ アクセス ポイントのプライマリ コントローラを確認します。

debug コマンド

次の 2 つのコマンドは、メッシュ アクセス ポイントとコントローラ間で交換されるメッセージを表示する場合にたいへん役立ちます。

```
(Cisco Controller) > debug capwap events enable
(Cisco Controller) > debug disable-all
```

debug コマンドを使用して、メッシュ アクセス ポイントとコントローラ間で行われるパケット交換のフローを表示できます。メッシュ アクセス ポイントで、検索プロセスが起動します。加入フェーズでクレデンシャルの交換が行われ、メッシュ アクセス ポイントがメッシュ ネットワークへの加入を許可されることが認証されます。

加入が正常に完了すると、メッシュ アクセス ポイントは CAPWAP 設定要求を送信します。コントローラは設定応答で応答します。メッシュアクセスポイントはコントローラからの設定応答を受信すると、各設定要素を評価し、それらを実装します。

リモート デバッグ コマンド

AP コンソール ポートへの直接接続またはコントローラのリモートデバッグ機能のいずれかによって、デバッグのために、メッシュ アクセス ポイント コンソールにログインできます。

コントローラでリモート デバッグを起動するには、次のコマンドを入力します。

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

AP コンソール アクセス

AP1500 にはコンソール ポートがあります。メッシュ アクセス ポイントにはコンソール ケーブルが付属していません。1550 シリーズのアクセス ポイントの場合、コンソール ポートは簡単にアクセスでき、アクセス ポイント ボックスを開く必要はありません。しかし、1520 シリーズの場合は、コンソール ポートにアクセスするには、メッシュ アクセス ポイントのヒンジ側を開け、補助ポートから外側にケーブルを引き出し、ラップトップに接続する必要があります。

AP1500 では、コードにコンソール アクセス セキュリティが埋め込まれており、コンソール ポートへの不正アクセスを防止し、セキュリティが拡張されています。

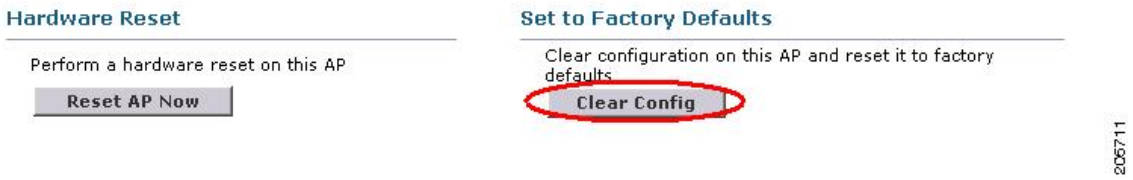
コンソール アクセス用の **ログイン ID** と**パスワード**はコントローラから設定します。次のコマンドを使用して、ユーザ名/パスワードの組み合わせを指定したメッシュ アクセス ポイントまたはすべてのアクセス ポイントに適用できます。

```
<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.

<Cisco Controller> config ap username cisco password cisco all
```

コントローラから適用されたユーザ名/パスワードがメッシュ アクセス ポイントのユーザ *ID* とパスワードとして使用されているか確認する必要があります。これは不揮発性設定です。ログイン *ID* とパスワードは、設定すると、メッシュ アクセス ポイントのプライベート設定に保存されます。

ログインに成功すると、トラップが Cisco Prime Infrastructure に送信されます。ユーザが 3 回連続してログインに失敗すると、ログイン失敗トラップがコントローラと Cisco Prime Infrastructure に送信されます。

注意 メッシュ アクセス ポイントは、別の場所に移動する前に、出荷時のデフォルト設定にリセットする必要があります。



AP からのケーブル モデムのシリアル ポート アクセス

コマンドは、CLI の特権モードからケーブル モデムに送信できます。コマンドを使用してテキスト文字列を取得し、ケーブル モデム UART インターフェイスに送信します。ケーブル モデムはそのテキスト文字列を独自のコマンドの 1 つとして解釈します。ケーブル モデムの応答が取得され、Cisco IOS コンソールに表示されます。ケーブル モデムからは、最大 9600 文字が表示されます。4800 文字を超えるテキストはすべて切り捨てられます。

モデムのコマンドは、元々ケーブル モデム用である UART ポートに接続されているデバイスがあるメッシュ AP でのみ使用できます。ケーブル モデムがない、または他のデバイスが UART に接続されているメッシュ AP でコマンドを使用した場合、コマンドは受け入れられますが、戻される出力は生成されません。明示的にフラグが付けられるエラーはありません。

設定

MAP の特権モードから次のコマンドを入力します。

`AP#`**send cmodem** *timeout-value modem-command*

modem コマンドは、ケーブルモデムに送信する任意のコマンドまたはテキストです。タイムアウト値の範囲は 1 ～ 300 秒です。ただし、取得されたデータが 9600 文字の場合、9600 文字を超え

るテキストは切り捨てられ、タイムアウト値とは関係なく、応答が AP コンソールにすぐに表示されます。

図 *3* : ケーブル モデム コンソールのアクセス コマンド

```
RAP-CM-N1#send ?
  *        All tty lines
  <0-16>   Send a message to a specific line
  cmodem   Enter cable modem command
  console  Primary terminal line
  log      Logging destinations
  vty      Virtual terminal

RAP-CM-N1#send cmodem ?
  LINE  Enter modem command string
  <cr>
```

279059

図 *4* : ケーブル モデム コンソールのアクセス コマンド

```
RAP-CM-N1#send cmodem ls
ls
CM>
CM> ls

!               ?               REM             cd              dir
find_command    help            history         instances       ls
man             pwd             sleep           syntax          system_time
usage
----
mbufShow        memShow         mutex_debug     ping            read_memory
reset           routeShow       run_app         shell           stackShow
start_idle_profiling            stop_idle_profiling             taskDelete
taskInfo        taskPrioritySet taskResume      taskShow        taskSuspend
taskTrace       usfsShow        version         write_memory    zone
----
[HeapManager] [SA] [cm_hal] [docsis_ctl] [embedded_target] [enet_hal]
[event_log] [flash] [forwarder] [ip_hal] [msgLog] [non-vol] [pingHelper]
[snmp] [snoop] [usb_hal]

CM>
RAP-CM-N1#send cmodem cd docsis
cd
CM>
CM> cd docsis
CM> cd docsis

Active Command Table:  CM DOCSIS Control Thread Commands (docsis_ctl)

CM -> docsis_ctl

CM/DocsisCtl>
RAP-CM-N1#
```

279060

注意 疑問符（?）と感嘆符（!）は、**send cmodem** コマンドでは使用できません。これらの文字は、Cisco IOS CLI で即座に別の意味に解釈されます。そのため、モデムに送信できません。

ケーブル モデム コンソール ポートの有効化

デフォルトでは、ケーブル モデム コンソール ポートは無効になります。これは、ユーザが自分の個人用のケーブル モデムを使用して、コンソールにアクセスできないようにするためです。AP1572IC、AP1572EC、AP1552C モデルでは、ケーブル モデム コンソールはアクセス ポイントに直接接続されます。コンソール ポートは、AP とケーブル モデムの間のシグナリングに必要です。SNMP を介して、または CMTS のコンフィギュレーション .cm ファイルにコマンドを追加して、ケーブル モデム コンソール ポートを有効にする 2 つの方法があります。

（注） AP1572EC、AP1572IC、AP1552C および AP1552CU の場合、ケーブル モデムを有効にする必要があります。

- ケーブル モデムの IP アドレスに次のコマンドを入力して、SNMP を介してケーブル モデム コンソール ポートを有効にします。
  ```
  snmpset -c private IP_ADDRESS cmConsoleMode.0 i N
  ```
  OID を使用して、次のコマンドを入力します。
  ```
  snmpset -c private IP_ADDRESS
  1.3.6.1.4.1.1429.77.1.4.7.0 i N
  ```
  IP_ADDRESS は任意の Ipv4 アドレス、N は整数、2 は読み取りと書き込みの有効化、1 は読み取り専用、0 は無効化です。

  例：
  ```
  snmpset -c private 209.165.200.224 cmConsoleMode.0 i 2
  ```

- コンフィギュレーション ファイルからケーブル モデム コンソール ポートを有効にします。コンフィギュレーション ファイル（.cm 拡張子）は、ケーブル モデム ヘッド エンドにロードされます。参加プロセスの一部としてケーブル モデムにプッシュされます。ケーブル モデム コンフィギュレーション ファイルに次の行を入力します。
  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```
  OID を使用して、この行を入力します。
  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```

ケーブル モデムを使用した AP1572xC/AP1552C のリセット

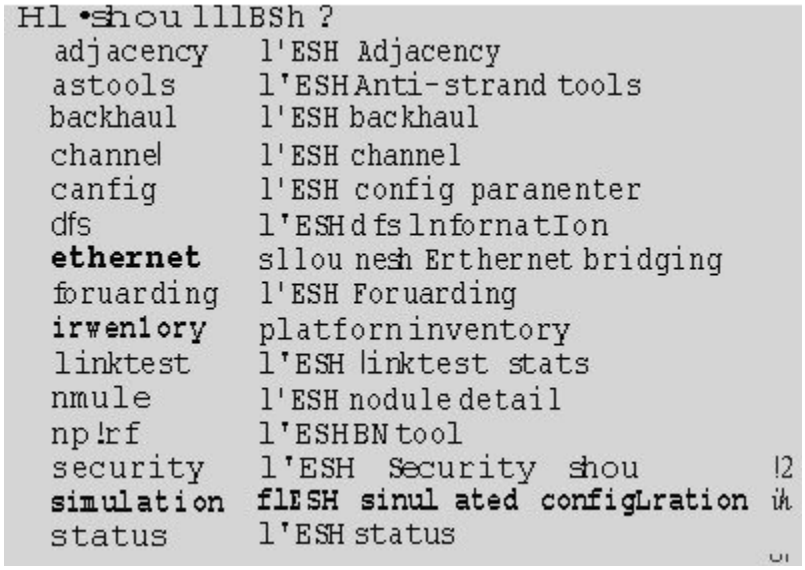
AP はアクセス ポイント内にあるケーブル モデムへ SNMP コマンドを入力してリセットできます。この機能を動作させるには、ケーブル モデム コンソール ポートを有効にする必要があります。

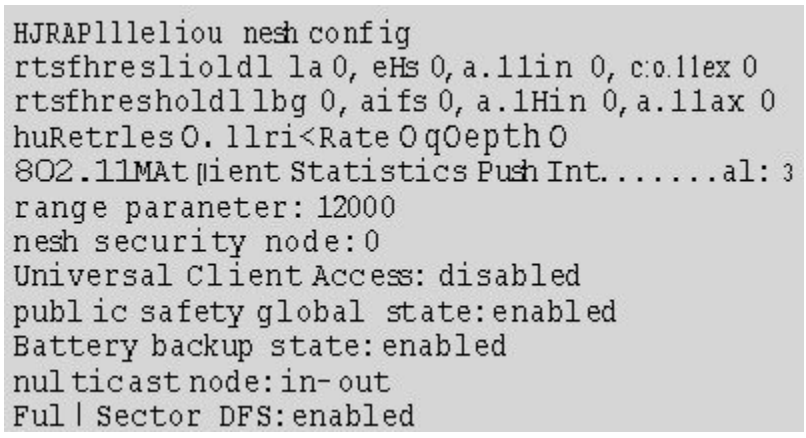
次の snmpset コマンドを入力して、AP をリセットします。
```
Snmpset -v2c -c public IP ADDRESS 1.3.6.1.4.1.1429.77.1.3.17.0 i 1
```

IP ADDRESS は、ケーブル モデムの IPv4 アドレスです。

メッシュ アクセス ポイント CLI コマンド

次のコマンドは、メッシュ アクセス ポイントで AP コンソール ポートを使用して直接入力できます。コントローラのリモート デバッグ機能を使用して入力することもできます。





```
HJRAPlllehou caplolBp client mb
Adnin5tate                          ADHIN ENABLED
SuVer                               S.2.98.0
NunFll ledSlots                     2
Nane                                HJRAPl
Location                            default location
Huarllame                           SEYf-CllffROLLER
Huarrlp                             209.165.200.227
Huartt.Ner                          0.0.0.0
ApHocle                              Brld!JE!
ApSubl'lode                         Not [:mf igured
OperationState                      UP
CAPllN'Path nru                      1485
Link!U:liting                       disabled
ApRole                              RootAP
ApBac:khaul                         802.l la
Ap8ac:khaulthannel                  5805
ApBac:khaulSl ot                    1
ApBac:khaul 11gEnabled              0
ApBac:l<haullxRate                  24000
Ethernet Brldglrg State             0
Public Safety State                 enabled
```

```
HJHAPlllehoi.I nesh adjacency ?
  alI      HESH Adjacency AlI
  child    HESH Adjacency Child
  parent MESH Adjacency Parent
                                    OI
```

```
HJMap4#shou mesh status '%
 shou MESH Status
 MeshAP in state Maint
 Uplink Backbone: Virtual-Dot11Radio0
 Downlink Backbone: Dot11Radio1
 Configured BGN: HuckJr
       rxNeighReq 129790 rxNeighRsp 66976 txNeighReq 33938 txNeighRsp 129790
       rxNeighRsp 1147275 txNeighUpd 202060
       nextchan 0 nextant 0 downAnt 0 downChan 0 curAnts 0
       nextNeigh 1. malformedNeighPackets 4.poorNeighSnr 1
       blacklistPackets 0,insufficientMemory 0, authenticationFailures 0
       Parent Changes 3, Neighbor Timeouts 0
       Vector through 0017.94fe.c3bf:
              Vector ease 1 -1, FWD: 0017.94fe.c3bf
                                                                    273949
```

```
HJNap4#show mesh forwarding link
 Current mesh links:
----------------------
 End Point  : 0017.94fe.c3bf
 Adjacency  : Exists
 Channel    : 161 on Dot11Radio1
 Type       : 2
 State      : 4
 Bundle     : member
 Bridge     : 1
 swidb      : Virtual-Dot11Radio0
 port state : OPEN
```

273950

メッシュ アクセス ポイント デバッグ コマンド

次のコマンドは、メッシュ アクセス ポイントで AP コンソール ポートを使用して直接入力しても、コントローラでリモート デバッグ機能を使用しても、入力できます。

- **debug mesh ethernet bridging**：イーサネット ブリッジをデバッグします。
- **debug mesh ethernet config**：VLAN タギングに関連付けられているアクセスおよびトランク ポート設定をデバッグします。
- **debug mesh ethernet registration**：VLAN 登録プロトコルをデバッグします。このコマンドは、VLAN タギングに関連付けられています。
- **debug mesh forwarding table**：ブリッジ グループを含む転送テーブルをデバッグします。
- **debugs mesh forwarding packet bridge-group**：ブリッジ グループ設定をデバッグします。

メッシュ アクセス ポイントのロール定義

デフォルトでは、AP1500 は MAP に設定された無線のロールで出荷されます。RAP として動作させるには、メッシュ アクセス ポイントを再設定する必要があります。

バックホール アルゴリズム

バックホールは、メッシュ アクセス ポイント間に無線接続だけを作成するために使用します。

デフォルトでバックホール インターフェイスは 802.11a です。バックホール インターフェイスを 802.11b/g に変更できません。

AP1500 には、デフォルトで「自動」データ レートが選択されています。

バックホール アルゴリズムは、孤立状態のメッシュ アクセス ポイントの状況に対処するために設計されました。このアルゴリズムは、各メッシュ ノードに高いレベルの復元力も追加します。

このアルゴリズムは、次のようにまとめることができます。

- MAP は常に、イーサネット ポートが UP の場合はイーサネット ポートを**プライマリ バックホール**として設定し、UP でない場合は 802.11a 無線として設定します（この機能により、ネットワーク管理者は、イーサネット ポートを最初に RAP として設定し、社内で回復する

ことができます）。ネットワークの高速コンバージェンスを可能にするため、メッシュ ネットワークへの最初の加入では、イーサネット デバイスを MAP に接続しないことを推奨します。

- UP であるイーサネット ポートで WLAN コントローラへの接続が失敗した MAP は 802.11a 無線を**プライマリ バックホール**として設定します。ネイバーの検索に失敗するか、802.11a 無線上でネイバーを経由した WLAN コントローラへの接続が失敗すると、イーサネット ポートで、再度**プライマリ バックホール**が UP になります。MAP は同じ BGN を持つ親を優先します。
- イーサネット ポートを介してコントローラに接続されている MAP は、（RAP とは違って）メッシュ トポロジをビルドしません。
- RAP は、常にイーサネット ポートを**プライマリ バックホール**として設定します。
- RAP のイーサネット ポートが DOWN の場合、または RAP が UP であるイーサネット ポートでコントローラに接続できない場合、802.11a 無線が**プライマリ バックホール**として設定されます。ネイバーの検索に失敗するか、802.11a 無線上でネイバーを経由したコントローラへの接続が失敗すると、15 分後に、RAP が SCAN 状態になり、イーサネット ポートが最初に起動します。

前述のアルゴリズムを使用して、メッシュ ノードの役割を保持すると、メッシュ アクセス ポイントが不明状態になり、ライブ ネットワークで孤立状態になるのを避けることができます。

パッシブ ビーコン（ストランディング防止）

パッシブ ビーコンをイネーブルにすると、孤立状態のメッシュ アクセス ポイントで、802.11b/g 無線を使用して、無線でそのデバッグ メッセージをブロードキャストできます。孤立状態のメッシュ アクセス ポイントをリッスンし、コントローラとの接続がある隣接メッシュ アクセス ポイントは、それらのメッセージを CAPWAP 経由でコントローラに渡します。パッシブ ビーコンにより、有線接続のないメッシュ アクセス ポイントが孤立状態になるのを防ぎます。

デバッグ ログもバックホール以外の無線で、救難ビーコンとして送信できるため、隣接メッシュ アクセス ポイントをビーコンのリッスン専用にすることができます。

メッシュアクセスポイントでコントローラへの接続が失われると、コントローラで次の手順が自動的に起動されます。

- 孤立状態のメッシュ アクセス ポイントの MAC アドレスを識別する
- CAPWAP が接続されているすぐ近くのネイバーを見つける
- リモート デバッグによってコマンドを送信する
- チャネルを循環してメッシュ アクセス ポイントを追跡する

この機能を使用するために、知っている必要があるのは孤立状態の AP の MAC アドレスだけです。

メッシュアクセスポイントは、孤立タイマーのリブートが実行された場合に孤立状態と見なされます。孤立タイマーのリブートが発生すると、現在孤立状態のメッシュアクセスポイントで、孤立防止機能のパッシブ ビーコンが有効になります。

この機能は 3 つの部分に分けられます。

- 孤立状態のメッシュ アクセス ポイントによる孤立検出
- 孤立状態のメッシュ アクセス ポイントによって送信されるビーコン
  - 802.11b 無線をチャネル（1、6、11）にラッチする
  - デバッグをイネーブルにする
  - 孤立デバッグ メッセージを救難ビーコンとしてブロードキャストする
  - 最新のクラッシュ情報ファイルを送信する
- ビーコンの受信（リモート デバッグがイネーブルになっている隣接メッシュ アクセス ポイント）

構成されたメッシュ アクセス ポイントは定期的に孤立状態のメッシュ アクセス ポイントを検索します。メッシュ アクセス ポイントは定期的に孤立状態のメッシュ アクセス ポイントのリストと SNR 情報をコントローラに送信します。コントローラはネットワーク内の孤立状態のメッシュ アクセス ポイントのリストを保持します。

debug mesh astools troubleshoot *mac-addr* **start** コマンドを入力すると、コントローラはリストを検索して、孤立状態のメッシュ アクセス ポイントの MAC アドレスを見つけます。

孤立状態のアクセス ポイントのリッスンを開始するメッセージが最適なネイバーに送信されます。リッスンしているメッシュ アクセス ポイントは、孤立状態のメッシュ アクセス ポイントからの救難ビーコンを取得し、コントローラに送信します。

メッシュ アクセス ポイントは、リスナーの役割を担うと、孤立状態のメッシュ アクセス ポイントのリッスンを停止するまで、孤立状態のメッシュアクセスポイントをその内部リストから消去しません。孤立状態のメッシュ アクセス ポイントのデバッグ中に、そのメッシュ アクセス ポイントのネイバーが一定の割合で、現在のリスナーより優れた SNR をコントローラに報告した場合、ただちに孤立状態のメッシュ アクセス ポイントのリスナーが新しいリスナー（SNR が優れた）に変更されます。

エンドユーザ コマンドは次のとおりです。

- **config mesh astools** [**enable** | **disable**]：メッシュ アクセス ポイントの astools をイネーブルまたはディセーブルにします。ディセーブルの場合、AP は孤立状態の AP リストをコントローラに送信しません。
- **show mesh astools stats**：孤立状態の AP とそれぞれのリスナー（存在する場合）のリストを表示します。
- **debug mesh astools troubleshoot** *mac-addr* **start**：最適なネイバーの *mac-addr* にメッセージを送信し、リッスンを開始します。

- **debug mesh astools troubleshoot** *mac-addr* **stop**：最適なネイバーの *mac-addr* にメッセージを送信し、リッスンを停止します。
- **clear mesh stranded** [**all** | *mac of b/g radio*]：孤立状態の AP エントリをクリアします。

コントローラ コンソールは、30 分間、孤立状態の AP からのデバッグ メッセージでいっぱいになります。

動的周波数選択（DFS）

以前は、レーダーを搭載するデバイスは、他の競合サービスがなく周波数サブバンドで動作していました。しかし、規制当局の管理により、これらの帯域をワイヤレス メッシュ LAN（IEEE 802.11）などの新しいサービスに開放して共有できるようにしようとしています。

既存のレーダー サービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要のあるデバイスに対して、動的周波数選択（DFS）プロトコルに従って動作することを求めています。DFS では、無線デバイスがレーダー信号の存在を検出できる機能の採用を義務付けています。無線がレーダー信号を検出すると、そのサービスを保護するために、少なくとも 30 分間送信を停止する必要があります。無線は、それをモニタした後にのみ送信されるように、別のチャネルを選択します。使用する予定のチャネルで少なくとも 1 分間レーダーが検出されなかった場合には、新しい無線サービス デバイスはそのチャネルで伝送を開始できます。

AP は 60 秒間新しい DFS チャネルで DFS スキャンを実行します。ただし、隣接する AP がその新しい DFS チャネルをすでに使用している場合、AP は DFS スキャンを実行しません。

無線がレーダー信号を検出して識別するプロセスは複雑なタスクであり、ときどきは誤った検出が起こります。誤った検出の原因には、RF 環境の不確実性や、実際のオンチャネル レーダーを確実に検出するためのアクセス ポイントの機能など、非常に多くの要因が考えられます。

802.11h 規格では、DFS および Transmit Power Control（TPC）について、5 GHz 帯域に関連するものと指定しています。DFS を使用してレーダーの干渉を回避し、TPC を使用して Satellite Feeder Link の干渉を回避します。

（注） DFS は、米国では 5250 ～ 5350 および 5470 ～ 5725 周波数帯域に義務付けられています。ヨーロッパでは、DFS と TPC が上記帯域に義務付けられています。

図 *5* : ***DFS*** および ***TPC*** 帯域の要件

RAP の DFS

RAP ではレーダー検出の応答として、次の手順が実行されます。

1. RAP が、チャネルがレーダーに影響を受けるコントローラにメッセージを送信します。チャネルが、RAP およびコントローラで影響を受けるチャネルとしてマークされます。
2. RAP がそのチャネルを 30 分間ブロックします。この 30 分間は非占有期間と呼ばれます。
3. コントローラが、チャネルでレーダーが検出されたことを示す TRAP を送信します。TRAP は非占有期間が経過するまで留まります。
4. RAP は 10 秒間でチャネルから移行します。これは、チャネル移行時間と呼ばれます。システムがチャネルをクリアする時間として定義され、レーダーバーストの終わりからチャネルの最終送信の終わりまで測定されます。
5. RAP が Quite モードに入ります。Quite モードで、RAP がデータ伝送を停止します。ビーコンは引き続き生成され、プローブ応答も引き続き配信されます。Quiet モードは、チャネル移行時間（10 秒）が終了するまで存続します。
6. コントローラが新しいランダム チャネルを選択し、チャネル情報を RAP に送信します。
7. RAP が新しいチャネル情報を受信し、チャネル変更フレーム（ユニキャスト、暗号化）を MAP に送信し、各 MAP が同じ情報をセクターの下位の子に送信します。各メッシュ アクセス ポイントは、100 ミリ秒ごとに 1 回ずつ合計 5 回、チャネル変更フレームを送信します。
8. RAP が新しいチャネルにチューニングし、サイレント モードになります。サイレント モード中は、レシーバだけが ON になります。RAP が新しいチャネルで、60 秒間レーダーの存在を

スキャンし続けます。このプロセスは、チャネル アベイラビリティ チェック（CAC）と呼ばれます。

9 MAP が新しいチャネルにチューニングし、サイレント モードになります。サイレント モード中は、レシーバだけが ON になります。MAP が新しいチャネルで、60 秒間レーダーの存在をスキャンし続けます。

10 レーダーが検出されない場合、RAP がこの新しいチャネルですべての機能を再開し、セクター全体がこの新しいチャネルにチューニングされます。

MAP の DFS

MAP ではレーダー検出の応答として、次の手順が実行されます。

1 MAP が、レーダー発見の指示を親と、最終的にそのチャネルが影響を受けることを示している RAP に送信します。RAP がこのメッセージをコントローラに送信します。このメッセージは、RAP から送信されたものであるように表示されます。MAP、RAP、およびコントローラが 30 分間影響を受けるものとしてチャネルをマークします。

2 MAP が 30 分間チャネルをブロックします。この 30 分間は非占有期間と呼ばれます。

3 コントローラが、チャネルでレーダーが検出されたことを示す TRAP を送信します。TRAP は非占有期間が経過するまで留まります。

4 MAP は 10 秒間でチャネルから移行します。これは、チャネル移行時間と呼ばれます。システムがチャネルをクリアする時間として定義され、レーダーバーストの終わりからチャネルの最終送信の終わりまで測定されます。

5 MAP が Quite モードに入ります。Quite モードで、MAP がデータ伝送を停止します。ビーコンは引き続き生成され、プローブ応答も引き続き配信されます。Quiet モードは、チャネル移行時間（10 秒）が終了するまで存続します。

6 コントローラが新しいランダム チャネルを選択し、チャネルを RAP に送信します。

7 RAP が新しいチャネル情報を受信し、チャネル変更フレーム（ユニキャスト、暗号化）を MAP に送信し、各 MAP が同じ情報をセクターの下位の子に送信します。各メッシュ アクセス ポイントは、100 ミリ秒ごとに 1 回ずつ合計 5 回、チャネル変更フレームを送信します。

8 各メッシュ アクセス ポイントが新しいチャネルにチューニングし、サイレント モードになります。サイレント モード中は、レシーバだけが ON になります。パケット伝送は行われません。AP が新しいチャネルで、60 秒間レーダーの存在をスキャンし続けます。このプロセスは、チャネル アベイラビリティ チェック（CAC）と呼ばれます。MAP はコントローラから切断されない必要があります。この 1 分間、ネットワークは安定した状態を維持する必要があります。

DFS 機能により、レーダー信号を検出した MAP はそれを RAP まで伝送することができ、RAP はレーダーを経験したことがあるかのように動作し、セクターを移動します。このプロセスは、コーディネイテッド チャネル変更と呼ばれます。コントローラで、この機能はオンまたはオフにできます。コーディネイテッド チャネル変更は、デフォルトでイネーブルになっています。

DFS をイネーブルにするには、次のコマンドを入力します。

```
(Cisco Controller) > config mesh full-sector-dfs enable
```

ネットワークで DFS がイネーブルになっているかどうかを確認するには、次のコマンドを入力します。

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

（注） レーダーを検出した MAP は、親の BGN が異ならない限り、RAP にメッセージを送信する必要があります。この場合、コーディネイテッド セクター変更のメッセージを送信しません。代わりに、MAP は再度 SCAN 状態になり、レーダーが発見されなかったチャネルで、新しい親を検索します。

（注） いずれのメッシュ アクセス ポイントもデフォルトの BGN を使用していないことを確認します。

（注） MAP で繰り返されたレーダー イベント（レーダーは 1 回トリガーすると、ほとんどすぐに再度トリガーする）により、MAP が切断されます。

DFS 環境での準備

この項では、DFS 環境での準備方法について説明します。

- コントローラが正しい国の地域に設定されていることを確認するには、次のコマンドを入力します。

  ```
  (Cisco Controller) > show country
  ```

- メッシュ アクセス ポイントの国とコントローラのチャネル設定を確認するには、次のコマンドを入力します。

  ```
  (Cisco Controller)> show ap config 802.11a ap-name
  ```

- メッシュに使用可能なチャネルを識別するには、次のコマンドを入力します。

  ```
  (Cisco Controller)> show ap config 802.11a ap-name
  ```

  許可されたチャネル リストを検索します。

  ```
  Allowed Channel List..................... 100,104,108,112,116,120,124,
  ..................................... 128,132,136,140
  ```

- AP コンソールで（またはコントローラからリモート デバッグを使用して）メッシュに使用可能なチャネルを識別するには、次のコマンドを入力します。

```
ap1520-rap # show mesh channels

HW: Dot11Radio1, Channels:
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
```

チャネルの横のアスタリスクは、チャネルでレーダーが検出されたことを示します。

- リモート デバッグを起動するには、次のコマンドを入力します。

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

- DFS チャネルのレーダー検出と過去のレーダー検出を確認するためのデバッグ コマンドは、次のようになります。

show mesh dfs channel *channel-number*
show mesh dfs history

以下のような情報が表示されます。

ap1520-rap # **show mesh dfs channel** 132

```
Channel 132 is available
Time elapsed since radar last detected: 0 day(s), 7 hour(s), 6 minute(s), 51 second(s).
```

RAP はすべてのチャネルを調べ、各チャネルにアクティブなレーダーがあるかどうかを判断する必要があります。

```
ap1520-rap # show mesh dfs channel 132

Radar detected on channel 132, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 7 minute(s), 11 second(s)).
Channel is set to 100 (Time Elapsed: 0 day(s), 7 hour(s), 7 minute(s), 11 second(s)).
Radar detected on channel 116, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 6 minute(s), 42 second(s)).
Channel is set to 64 (Time Elapsed: 0 day(s), 7 hour(s), 6 minute(s), 42 second(s)).
Channel 132 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 37 minute(s), 10
second(s)).
Channel 116 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 36 minute(s), 42
second(s)).
```

DFS のモニタ

DFS 履歴は、レーダーを検出するために、毎朝、またはより頻繁に実行する必要があります。この情報は消去されず、メッシュ アクセス ポイントのフラッシュに保存されます。そのため、ユーザは時間を合わせるだけで済みます。

```
ap1520-rap # show controller dot11Radio 1
```

以下に類似した情報が表示されます。

```
interface Dot11Radio1
```

```
Radio Hammer 5, Base Address 001c.0e6c.9c00, BBlock version 0.00, Software version 0.05.30
Serial number: FOC11174XCW
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: ETSI (OFDM) (EU) (-E)
Uniform Spreading Required: Yes
Current Frequency: 5540 MHz Channel 108 (DFS enabled)
Allowed Frequencies: *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *560
0(120) *5620(124) *5640(128) *5660(132) *5680(136) *5700(140)
* = May only be selected by Dynamic Frequency Selection (DFS)
Listen Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(6
0) 5320(64) 5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5660(132) 5680(136
) 5700(140) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165) 4950(20) 4955(21)
4960(22) 4965(23) 4970(24) 4975(25) 4980(26)
```

（注） アスタリスクは、このチャネルで DFS がイネーブルになっていることを示します。

周波数プランニング

隣接セクターの代替隣接チャネルを使用します。同じ場所に 2 つの RAP を展開する場合、それらの間に 1 つのチャネルを残しておく必要があります。

気象レーダーは 5600 ～ 5650 MHz 帯域で動作します。つまり、チャネル 124 および 128 が影響を受ける可能性があり、チャネル 120 と 132 も気象レーダーの活動に影響を受ける可能性があります。

メッシュ アクセス ポイントがレーダーを検出すると、コントローラとメッシュ アクセス ポイントは共にチャネルを設定されたチャネルとして保持します。コントローラはそれをメッシュ アクセス ポイントに関連付けられた揮発性メモリに保存し、メッシュ アクセス ポイントはそれを設定としてフラッシュに保存します。30 分の Quiet 時間後、コントローラは、メッシュ アクセス ポイントが新しいチャネルで設定されているかどうかに関係なく、メッシュアクセスポイントをスタティック値に戻します。これを避けるには、メッシュアクセスポイントを新しいチャネルで設定し、メッシュ アクセス ポイントをリブートします。

あるチャネルでレーダーが確実に検出されたら、次のように、そのチャネルおよび周囲の 2 つのチャネルを RRM 除外リストに追加する必要があります。

```
(Cisco Controller) > config advanced 802.11a channel delete channel
```

メッシュ アクセス ポイントは RRM によって選択された新しいチャネルに移行し、除外されたチャネルを考慮しません。

たとえば、チャネル 124 でレーダーが検出された場合、チャネル 120、124、および 128 を除外リストに追加する必要があります。さらに、RAP をそれらのチャネルで動作しないように設定します。

適切な信号対雑音比

ヨーロッパのインストールでは、信号対雑音比（SNR）の最小の推奨値が 20 dB に増えます。追加の dB は、DFS 以外の環境で検出されないパケット受信へのレーダー干渉の影響を緩和するために使用されます。

アクセス ポイントの配置

メッシュ アクセス ポイントのコロケーションには、最低 10 フィート（3.048 m）の垂直区切り、または 100 フィート（30.48 m）の水平区切りが必要です。

パケット エラー率のチェック

1 % 以上のエラー率が高いメッシュ アクセス ポイントには、ノイズと干渉に使用されるチャネルを変更するか、伝送パスに追加のメッシュ アクセス ポイントを追加して、メッシュ アクセス ポイントを別のセクターに移動するか、またはメッシュ アクセス ポイントを追加することによって、緩和策を適用する必要があります。

ブリッジ グループ名の誤った設定

メッシュ アクセス ポイントに、*bridgegroupname* が誤って指定され、意図されないグループに配置されることがあります。ネットワーク設計によっては、このメッシュアクセスポイントに到達して、その正しいセクターやツリーを見つけられたり、見つけられなかったりする可能性があります。メッシュアクセスポイントが互換性のあるセクターに到達できない場合、孤立状態になる可能性があります。

孤立状態のメッシュ アクセス ポイントを回復するために、デフォルトの bridgegroupname の概念がソフトウェアに導入されています。メッシュ アクセス ポイントは、設定された bridgegroupname を使用して他のメッシュ アクセス ポイントに接続できない場合、デフォルトの bridgegroupname を使用して接続を試みます。

この孤立状況の検出と回復のアルゴリズムは、次のようになります。

1. パッシブ スキャンを実行し、bridgegroupname に関係なく、すべてのネイバー ノードを検出します。
2. メッシュ アクセス ポイントは、AWPP を使用して、*my own bridgegroupname* でリッスンしたネイバーに接続します。
3. 手順 2 が失敗した場合、AWPP を使用して、デフォルトの bridgegroupname で接続を試みます。
4. 手順 3 で失敗した試行ごとに、ネイバーが除外リストに追加され、次の最適なネイバーへの接続が試行されます。
5. 手順 4 で AP がすべてのネイバーへの接続を失敗した場合、メッシュ アクセス ポイントがリブートされます。
6. 15 分間、デフォルトの bridgegroupname で接続した場合、メッシュ アクセス ポイントはスキャン状態になります。

メッシュ アクセス ポイントがデフォルトの bridgegroupname で接続できた場合、親ノードは、メッシュ アクセス ポイントをコントローラのデフォルトの子/ノード/ネイバー エントリとして報告するため、ネットワーク管理者は Cisco Prime Infrastructure になります。そのようなメッシュ アクセ

スポイントは通常の（非メッシュ）アクセスポイントとして動作し、すべてのクライアントを受け入れ、他のメッシュ ノードをその子とし、すべてのデータ トラフィックを通します。

（注） DEFAULT の未割り当ての BGN（NULL 値）と混同しないでください。これは、アクセス ポイントで独自の BGN を見つけられない場合に、接続に使用されるモードです。

メッシュ アクセス ポイントの BGN の現在の状態を確認するには、次のコマンドを入力します。

```
(Cisco Controller)> show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 48, linkSnr
 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B) snrUp 72, snrDown 63, linkSrn 57
00:0B:85:5F:FA:60 is RAP
```

メッシュ アクセス ポイントの BGN の現在の状態を確認し、メッシュ アクセス ポイントのネイバー情報を確認するには、次の手順を実行します（GUI）。

[Wireless] > [All APs] > [AP Name] > [Neighbor info] を選択します。

図 *6*：子のネイバー情報

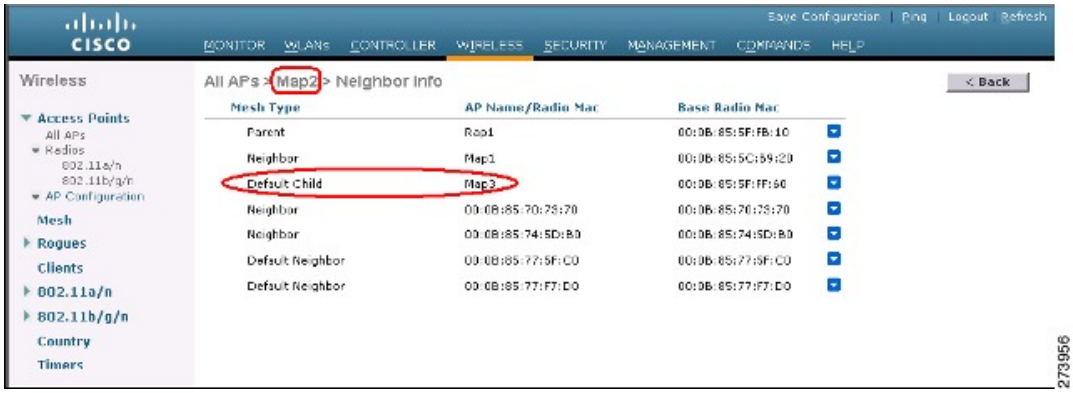


図 *7*：親のネイバー情報

メッシュ アクセス ポイントの IP アドレスの誤った設定

ほとんどのレイヤ 3 ネットワークは DHCP IP アドレス管理を使用して導入されますが、一部のネットワーク管理者は IP アドレスを手動で管理し、各メッシュ ノードに IP アドレスを静的に割り当てることを好みます。手動でのメッシュ アクセス ポイントの IP アドレスの管理は、大規模なネットワークでは悪夢になりかねませんが、小規模から中規模のネットワーク（10 ～ 100 メッシュ ノード程度）では、メッシュ ノードの数がクライアント ホスト数と比べてかなり少ないので道理にかなっています。

メッシュ ノードに IP アドレスをスタティックに設定すると、サブネットや VLAN などの誤ったネットワークに MAP を配置してしまう可能性があります。この誤りにより、メッシュ アクセス ポイントで、IP ゲートウェイを正しく解決できなくなり、WLAN コントローラを検出できなくなる可能性があります。そのようなシナリオでは、メッシュ アクセス ポイントがその DHCP メカニズムにフォールバックし、自動的に DHCP サーバを見つけて、IP アドレスを取得しようとします。このフォールバック メカニズムにより、誤って設定されたスタティック IP アドレスから、メッシュ ノードが孤立する可能性を回避し、ネットワーク上の DHCP サーバから正しいアドレスを取得できます。

手動で IP アドレスを割り当てる場合、最初に最も遠いメッシュ アクセス ポイントの子から IP アドレッシングを変更し、RAP まで戻ってくることを推奨します。これは、装置を移動する場合にも当てはまります。たとえば、メッシュアクセスポイントをアンインストールし、異なるアドレスが設定されたサブネットを持つメッシュ ネットワークの別の物理的場所に再展開する場合などです。

別のオプションは、RAP と共にレイヤ 2 モードのコントローラを、誤って設定された MAP がある場所に運ぶことです。設定変更が必要な MAP に一致するブリッジ グループ名を RAP に設定します。MAP の MAC アドレスをコントローラに追加します。メッシュ アクセス ポイントの概要詳細に、誤って設定された MAP が表示されたら、それを IP アドレスで設定します。

DHCP の誤った設定

DHCP フォールバック メカニズムがあっても、次のいずれかの状況が存在する場合に、メッシュ アクセス ポイントが孤立する可能性があります。

- ネットワークに DHCP サーバがない
- ネットワークに DHCP サーバがあるが、AP に IP アドレスを提供しないか、AP に誤った IP アドレスを提供している場合（誤った VLAN またはサブネット上など）。

こうした状況によって、誤ったスタティック IP アドレスで設定されているか、設定されていないか、または DHCP で設定されているメッシュ アクセス ポイントが孤立する可能性があります。このため、すべての DHCP 検出の試行回数、DHCP 再試行回数、または IP ゲートウェイ解決再試行回数を試しても接続できない場合、メッシュ アクセス ポイントがレイヤ 2 モードでコントローラの検出を試みることを確認する必要があります。言い換えると、メッシュ アクセス ポイントは、最初にレイヤ 3 モードでコントローラの検出を試み、このモードでスタティック IP（設定されている場合）と DHCP（可能な場合）の両方で試みます。次に、AP はレイヤ 2 モードで、コント

ローラの検出を試みます。レイヤ 3 およびレイヤ 2 モードの試行を何回か試みたら、メッシュ アクセス ポイントはその親ノードを変更し、DHCP 検出を再試行します。さらに、ソフトウェア除外リストに、正しい IP アドレスを取得できなかった親ノードが記載されます。

ノード除外アルゴリズムについて

メッシュ ネットワークの設計によっては、ノードがそのルーティング メトリックに従って、再帰的に真の場合でも、別のノードを「最適」だと判断することがありますが、ノードに正しいコントローラや正しいネットワークへの接続を提供することはできません。これは、誤った配置、プロビジョニング、ネットワークの設計のいずれかによって、または特定のリンクの AWPP ルーティング メトリックを、永続的または一時的な方法で最適化する状況を示す RF 環境の動的な性質によって、発生する典型的なハニーポットアクセスポイントのシナリオです。ほとんどのネットワークで、そのような状況の回復は一般に難しく、ノードを完全にブラックホール化またはシンクホール化し、ネットワークから除外させる可能性があります。次の現象が見られる場合がありますが、これらに限定されるわけではありません。

- ハニーポットにノードが接続しているが、静的 IP アドレスが設定されている場合に IP ゲートウェイが解決できない、または DHCP サーバから正しい IP アドレスが取得できない、あるいは WLAN コントローラに接続できない。
- いくつかの、または（最悪の場合）多数のハニーポット間をノードが循環している。

シスコのメッシュ ソフトウェアは、高度なノード除外リストアルゴリズムを使用してこの困難なシナリオを解決します。このノード除外リストアルゴリズムは、指数バックオフ、および TCP スライディング ウィンドウや 802.11 MAC などの高度な技術を使用します。

基本なアイデアは次の 5 つの手順に基づいています。

1. ハニーポットの検出：次の手順でハニーポットが最初に検出されます。

   次を試行することにより、AWPP モジュールによって親ノードが設定されます。

   - CAPWAP モジュールの固定 IP アドレス
   - DHCP モジュールの DHCP
   - CAPWAP による障害が発生したコントローラの検出および接続

2. ハニーポットの確定：ハニーポットが検出されると、それが確定されるまでの期間、除外リストのデータベースに配置されます。デフォルト値は 32 分です。その後、現在のメカニズムに障害が発生すると次にフォールバックされ、次の順序で他のノードが親になるよう試行されます。

   - 同じチャネル
   - 別のチャネル（最初は独自のブリッジグループ名を持つチャネル、次にデフォルトのチャネル）
   - 現在のすべての除外リストのエントリの確定をクリアした、別のサイクル
   - AP のリブート

3 非ハニーポットの信用：ノードが実際にはハニーポットではないにもかかわらず、次のような一時的なバックエンド状態によってハニーポットとして表示されることがよくあります。

- DHCP サーバが、起動して実行していないか、一時的に障害が発生している、あるいはリブートが必要な状態
- WLAN コントローラが、起動して実行していないか、一時的に障害が発生している、あるいはリブートが必要な状態
- RAP 上のイーサネット ケーブルが誤って外れている状態

このような非ハニーポットは、ノードができるだけ早くサービス状態に戻れるように正しく信用される必要があります。

4 ハニーポットの期限：期限に達すると、除外リストのノードは除外リストのデータベースから削除され、AWPP によって今後のために通常の状態に戻る必要があります。

5 ハニーポットのレポート：コントローラへの LWAPP のメッシュ ネイバー メッセージを介してコントローラにハニーポットがレポートされます。レポートは [Bridging Information] ページに表示されます。メッセージは、最初に除外リストに記載されたネイバーが見られた際にも表示されます。後続のソフトウェア リリースでは、このような状況が発生した場合、コントローラで SNMP トラップが生成され、Cisco Prime Infrastructure で記録できるようになります。

図 *8*：除外ネイバー

多くのノードは予定のイベントまたは予定外のイベント後にネットワークに加入または再加入を試みる可能性があるので、16 分のホールドオフ時間が実装されます。これは、システム初期化後、16 分間はノードが除外リストに追加されないことを意味します。

この指数バックオフおよび高度なアルゴリズムは独特であり、次のプロパティがあります。

- 親ノードが本当にハニーポットなのか、それとも一時的に機能が停止しているだけなのかをノードによって正しく判断できるようにします。
- ノードのネットワークへの接続が維持された時間に基づいて、良好な親ノードであると信用します。信用することで、本当に一時的な状況の場合は除外リストの確定時間をきわめて短くすることができ、中程度の機能停止の場合は適度にすることができます。

- 組み込みのヒステリシス機能があります。これは、多くのノードが同じネットワーク内に存在しないかどうか互いのノードの検出を試みている場所で初期状態の問題が発生した場合に使用されます。
- 組み込みメモリがあります。これは、除外リストデータベースでかつて親ノードとして登録されていた場合（あるいは今後親ノードになる場合）、現在誤って親ノードと見なされないように、時々ネイバーになり得るノードに使用されます。

ノード除外リストアルゴリズムは、メッシュネットワークの重大な孤立を防ぎます。このアルゴリズムは、ノードが迅速に再コンバージェンスして、正しいネットワークを探すことができる方法で AWPP に統合されます。

スループット分析

スループットはパケット エラー レートおよびホップ カウントによって決まります。

容量とスループットは直交概念です。スループットはノード N でのユーザ エクスペリエンスです。領域の合計容量はN個のノードの全体のセクターで計算され、入力および出力RAP数に基づいています。また個別の妨害チャネルがないことを想定しています。

たとえば、10 Mbps での 4 つの RAP はそれぞれ合計容量 40 Mbps を配信します。1 ユーザが 2 つのホップを経由する場合、論理的には各 RAP で TPUT ごとに 5 Mbps を受信できることになり、40 Mbps のバックホール容量を消費します。

Cisco Mesh ソリューションを使用する場合、ホップごとの遅延は 10 ミリ秒未満で、ホップごとの遅延の範囲は標準で 1 ～ 3 ミリ秒です。ジッタ全体も 3 ミリ秒未満になります。

スループットは、ユーザ データグラム プロトコル（UDP）または Transmission Control Protocol（TCP）という、ネットワークを通過するトラフィックのタイプによって決まります。UDPはイーサネット経由で送信元アドレスおよび送信先アドレスを持つパケットおよびUDP プロトコルのヘッダーを送信します。確認応答（ACK）は行われません。パケットがアプリケーション層で配信されるかどうかは保証されません。

TCP は UDP と似ていますが、信頼性のあるパケット配信メカニズムです。パケットの ACK が行われ、スライディング ウィンドウ技術を使用することによって ACK を待つ前に送信者が複数のパケットを送信できます。クライアントが送信するデータの最大量が決められています（TCP ソケットバッファ ウィンドウと呼びます）。シーケンス番号により、送信したパケットを追跡し、パケットを正しい順序で到着させることができます。TCPは累積的にACKを使用し、現在どのくらいのストリームが受信されたかを受信側がレポートします。ACK は TCP のウィンドウ サイズ内であればいくつでもパケットを扱うことができます。

TCP はスロー スタートおよび乗法減少を使用してネットワーク輻輳やパケット損失に対応します。パケットが損失すると TCP ウィンドウは半分になり、バックオフ再送信タイマーが急激に増加します。ワイヤレスはインターフェイスの問題によりパケット損失の影響を受けますが、TCP はこのパケット損失に応答します。パケット損失からリカバリする際に接続が切断されないように、スロー スタート リカバリ アルゴリズムも使用されます。これらのアルゴリズムは、損失の多いネットワーク環境でトラフィック ストリーム全体のスループットを減少させる効果があります。

デフォルトでは、TCP の最大セグメント サイズ（MSS）は 1460 バイトで、1500 バイトの IP データグラムになります。TCP は 1460 バイトを超えるデータ パケットを分割し、スループットが少なくとも 30 % 減少します。さらに図 9：CAPWAP でトンネリングされたパケット，（24 ページ）に示されているように、コントローラによって IP データグラムが 48 バイトの CAPWAP トンネル ヘッダーにカプセル化されます。1394 バイトを超えるデータ パケットもコントローラによって分割され、スループットが最大 15 % 減少します。

図 *9*：*CAPWAP* でトンネリングされたパケット