モニタリングとモビリティの検証

モビリティ ping テストの実行

モビリティ ping テストについて

1 つのモビリティ リスト内のコントローラは、well-known UDP ポート上で情報を制御し、Ethernet-over-IP（EoIP）トンネルを通じてデータ トラフィックを交換することにより、お互いに通信します。UDP と EoIP は信頼できる転送メカニズムではないため、モビリティ コントロール パケットまたはデータ パケットがモビリティ ピアに配信される保証はありません。ファイアウォールによる UDP ポートや EoIP パケットのフィルタリング、あるいはルーティングの問題のために、モビリティ パケットが転送中に消失する可能性があります。

モビリティ ping テストの制約事項

- モビリティ ping テストを実行して、モビリティ通信環境をテストできます。これらのテストを使用して、モビリティ グループ（ゲスト コントローラを含む）のメンバ間の接続を検証できます。次の 2 つの ping テストが利用できます。
  - UDP でのモビリティ ping：このテストは、モビリティ UDP ポート 16666 上で実行されます。このテストでは、管理インターフェイスを介してモビリティ制御パケットが到達できるかどうかを確認します。
  - EoIP 経由のモビリティ ping：このテストは EoIP 経由で実行されます。管理インターフェイス上で、モビリティ データ トラフィックをテストします。
- 各コントローラにつき、実行できるモビリティ ping テストは 1 度に 1 回だけです。
- これらの ping テストは、インターネット制御メッセージ プロトコル（ICMP）ベースではありません。「ping」という用語は、エコー要求とエコー応答メッセージを示すために使用されます。

（注） ICMP パケットが 1280 バイトより大きい場合は、常に応答には 1280 バイトに切り詰められたパケットが使用されます。たとえば、ホストから管理インターフェイスに 1280 バイトを超えるパケットを使用して ping すると、常に 1280 バイトに切り詰められたパケットが使用されます。

- ポート 16666 および 16667 に対するモビリティ ping は注目すべき例外で、これらのポートは ACL によってブロックできません。

モビリティ ping テストの実行（CLI）

手順

ステップ 1 2 つのコントローラ間でモビリティ UDP コントロール パケット通信をテストするには、次のコマンドを入力します。

mping *mobility_peer_IP_address*

mobility_peer_IP_address パラメータは、モビリティ リストに属するコントローラの IP アドレスにする必要があります。

ステップ 2 2 つのコントローラ間でモビリティ EoIP データ パケット通信をテストするには、次のコマンドを入力します。

eping *mobility_peer_IP_address*

mobility_peer_IP_address パラメータは、モビリティ リストに属するコントローラの IP アドレスにする必要があります。

ステップ 3 モビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

config logging buffered debugging

show logging

ステップ 4 UDP でのモビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

debug mobility handoff enable

（注） トラブルシューティングを行う際には、Ethereal トレース キャプチャを使用することをお勧めします。

WLAN モビリティ セキュリティの値について

すべてのアンカーまたはモビリティのイベントでは、各コントローラの WLAN セキュリティ ポリシーの値は一致する必要があります。これらの値はコントローラのデバッグで検証することができます。次の表に、WLAN モビリティ セキュリティの値と対応するセキュリティ ポリシーを示します。

表 *1 : WLAN* モビリティ セキュリティの値

セキュリティの 16 進数値	セキュリティ ポリシー
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed （注） ソフトウェア リリース 6.0 以降を実行しているコントローラは、このセキュリティ ポリシーをサポートしていません。
0x00001000	Security_Web_Passthrough