システム ロギングとメッセージ ロギング

- システム ロギングとメッセージ ロギングについて （1 ページ）
- デバッグ ファシリティの使用方法 （10 ページ）

システム ロギングとメッセージ ロギングについて

システム ロギングを使用すると、コントローラのシステム イベントを最大 3 台のリモート syslog サーバにログできるようになります。syslog メッセージはコントローラに設定されている syslog サーバごとにログされるため、コントローラは各 syslog メッセージのコピーを送信します。複数のサーバに syslog メッセージを送信できるため、1 台の syslog サーバが一時的に使用できなくなってもメッセージが失われることがありません。メッセージ ロギングを使用すると、システム メッセージをコントローラのバッファまたはコンソールにログできるようになります。

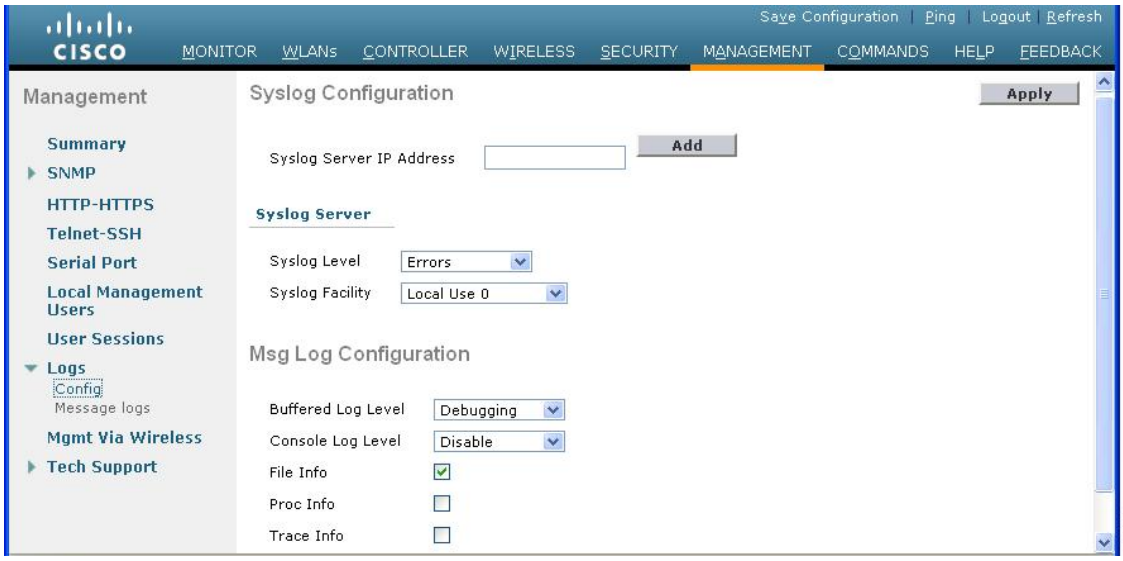
システム メッセージとトラップ ログの詳細については、http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-system-message-guides-list.htmlを参照してください。

システム ロギングとメッセージ ロギングの設定（GUI）

手順

ステップ 1 [Management] > [Logs] > [Config] の順に選択します。[Syslog Configuration] ページが表示されます。

図 *1 : [Syslog Configuration]* ページ



ステップ 2 [Syslog Server IPv4/IPv6 Address] テキスト ボックスに、syslog メッセージの送信先となるサーバの IPv4/IPv6 IP アドレスを入力し、[Add] をクリックします。コントローラには最大 3 台の syslog サーバを追加できます。このテキストボックスの下には、すでにコントローラに追加されている syslog サーバのリストが表示されます。

（注） コントローラから syslog サーバを削除するには、目的のサーバの右側の [Remove] をクリックします。

ステップ 3 syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、[Syslog Level] ドロップダウン リストから次のいずれかのオプションを選択します。

- [Emergencies] = 重大度レベル 0
- [Alerts] = 重大度レベル 1（デフォルト値）
- [Critical] = 重大度レベル 2
- [Errors] = 重大度レベル 3
- [Warnings] = 重大度レベル 4
- [Notifications] = 重大度レベル 5
- [Informational] = 重大度レベル 6
- [Debugging] = 重大度レベル 7

syslog レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、syslog サーバに送信されます。たとえば、syslog レベルを [Warnings]（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしか syslog サーバに送信されません。

（注） ロギング バッファへのデバッグ メッセージのロギングを有効にした場合は、アプリケーションデバッグからの一部のメッセージが、設定したレベルよりも上の重大度でメッセージ ログに表示されることがあります。たとえば、**debug client** *mac addr* コマンド実行した場合、メッセージの重大度レベルが [Errors] に設定されている場合でも、クライアント イベント ログがメッセージ ログに表示されることがあります。

ステップ 4 syslog メッセージを syslog サーバに送信するファシリティを設定するには、[Syslog Facility] から次のいずれかのオプションを選択します。 ドロップダウン リスト

- [Kernel] = ファシリティ レベル 0
- [User Process] = ファシリティ レベル 1
- [Mail] = ファシリティ レベル 2
- [System Daemons] = ファシリティ レベル 3
- [Authorization] = ファシリティ レベル 4
- [Syslog] = ファシリティ レベル 5（デフォルト値）
- [Line Printer] = ファシリティ レベル 6
- [USENET] = ファシリティ レベル 7
- [Unix-to-Unix Copy] = ファシリティ レベル 8
- [Cron] = ファシリティ レベル 9
- [FTP Daemon] = ファシリティ レベル 11
- [System Use 1] = ファシリティ レベル 12
- [System Use 2] = ファシリティ レベル 13
- [System Use 3] = ファシリティ レベル 14
- [System Use 4] = ファシリティ レベル 15
- [Local Use 0] = ファシリティ レベル 16
- [Local Use 2] = ファシリティ レベル 17
- [Local Use 3] = ファシリティ レベル 18
- [Local Use 4] = ファシリティ レベル 19
- [Local Use 5] = ファシリティ レベル 20
- [Local Use 5] = ファシリティ レベル 21
- [Local Use 5] = ファシリティ レベル 22
- [Local Use 5] = ファシリティ レベル 23

ステップ 5 [Apply] をクリックします。

ステップ 6 コントローラのバッファとコンソールに対するロギング メッセージの重大度レベルを設定するには、[Buffered Log Level] ドロップダウン リストおよび [Console Log Level] ドロップダウン リストから次のいずれかのオプションを選択します。

- [Emergencies] = 重大度レベル 0
- [Alerts] = 重大度レベル 1

- [Critical] = 重大度レベル 2
- [Errors] = 重大度レベル 3（デフォルト値）
- [Warnings] = 重大度レベル 4
- [Notifications] = 重大度レベル 5
- [Informational] = 重大度レベル 6
- [Debugging] = 重大度レベル 7
- [Disable]：このオプションは、コンソール ログ レベルの場合にのみ使用できます。このオプションを選択すると、コンソール ロギングが無効になります。

ロギング レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ロギング レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしかログされません。

ステップ 7 ソース ファイルの情報をメッセージ ログに含める場合は、[File Info] チェックボックスをオンにします。デフォルト値はイネーブルです。

ステップ 8 トレースバック情報をメッセージ ログに含める場合は、[Trace Info] チェックボックスをオンにします。デフォルトではディセーブルになっています。

ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

メッセージ ログの表示（GUI）

コントローラの GUI を使用してメッセージ ログを表示するには、[Management] > [Logs] > [Message Logs] の順に選択します。[Message Logs] ページが表示されます。

（注） コントローラから現在のメッセージ ログをクリアするには、[Clear] をクリックします。

システム ロギングとメッセージ ロギングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、システム ロギングを有効にし、syslog メッセージの送信先である syslog サーバの IP アドレスを設定します。

config logging syslog host *server_IP_address*

コントローラには最大 3 台の syslog サーバを追加できます。

（注） コントローラから syslog サーバを削除するには、**config logging syslog host** *server_IP_address* **delete** コマンドを入力します。

ステップ 2 次のコマンドを入力して、syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定します。

config logging syslog level *severity_level*

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注） 代わりに、*severity_level* パラメータに 0 ～ 7 の数を入力することもできます。

（注） syslog レベルを設定する場合は、重大度がそのレベル以下であるメッセージだけが syslog サーバに送信されます。たとえば、syslog レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしか syslog サーバに送信されません。

ステップ 3 次のコマンドを入力して、特定のアクセス ポイントまたはすべてのアクセス ポイントに対する syslog メッセージのフィルタリングの重大度レベルを設定します。

config ap logging syslog level *severity_level* {*Cisco_AP* | **all**}

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注） syslog レベルを設定する場合は、重大度がそのレベル以下のメッセージだけがアクセス ポイントに送信されます。たとえば、syslog レベルを警告（重大度 4）に設定した場合は、重大度が 0 ～ 4 のメッセージだけがアクセス ポイントに送信されます。

ステップ 4 次のコマンドを入力して、syslog サーバへ発信する syslog メッセージのファシリティを設定します。

config logging syslog facility *facility-code*

facility-code は、次のいずれかです。

- ap = AP 関連トラップ。
- authorization = 認可システム。ファシリティ レベル = 4。
- auth-private = 認可システム（プライベート）。ファシリティ レベル = 10。
- cron = cron/at ファシリティ。ファシリティ レベル = 9。
- daemon = システム デーモン。ファシリティ レベル = 3。
- ftp = FTP デーモン。ファシリティ レベル = 11。
- kern = カーネル。ファシリティ レベル = 0。
- local0 = ローカル使用。ファシリティ レベル = 16。
- local1 = ローカル使用。ファシリティ レベル = 17。
- local2 = ローカル使用。ファシリティ レベル = 18。
- local3 = ローカル使用。ファシリティ レベル = 19。
- local4 = ローカル使用。ファシリティ レベル = 20。
- local5 = ローカル使用。ファシリティ レベル = 21。
- local6 = ローカル使用。ファシリティ レベル = 22。
- local7 = ローカル使用。ファシリティ レベル = 23。
- lpr = ライン プリンタ システム。ファシリティ レベル = 6。
- mail = メール システム。ファシリティ レベル = 2。
- news = USENET ニュース。ファシリティ レベル = 7。
- sys12 = システム使用。ファシリティ レベル = 12。
- sys13 = システム使用。ファシリティ レベル = 13。
- sys14 = システム使用。ファシリティ レベル = 14。
- sys15 = システム使用。ファシリティ レベル = 15。
- syslog = syslog 自体。ファシリティ レベル = 5。
- user = ユーザ プロセス。ファシリティ レベル = 1。
- uucp = UNIX 間コピー システム。ファシリティ レベル = 8。

ステップ 5 次のコマンドを使用して AP の syslog ファシリティを設定します。

config logging syslog facility *AP*

AP には、次のいずれかを指定できます。

- associate = AP の関連付け syslog
- disassociate= AP の関連付け解除 syslog

ステップ 6 次のコマンドを入力して、1 つの AP またはすべての AP の syslog 機能を設定します。

config ap logging syslog facility *facility-level* {*Cisco_AP* | **all**}

facility-level は、次のいずれかです。

- auth = 認証システム
- cron = cron/at ファシリティ

- daemon = システム デーモン
- kern = カーネル
- local0 = ローカル使用
- local1 = ローカル使用
- local2 = ローカル使用
- local3 = ローカル使用
- local4 = ローカル使用
- local5 = ローカル使用
- local6 = ローカル使用
- local7 = ローカル使用
- lpr = ライン プリンタ システム
- mail = メール システム
- news = USENET ニュース
- sys10 = システム使用
- sys11 = システム使用
- sys12 = システム使用
- sys13 = システム使用
- sys14 = システム使用
- sys9 = システム使用
- syslog = syslog 自体
- user = ユーザ プロセス
- uucp = UNIX 間コピー システム

ステップ 7 次のコマンドを入力して、クライアントの syslog 機能を設定します。

config logging syslog facility クライアント

facility-code には、次のいずれかを指定できます。

- assocfail Dot11= クライアントの関連付け失敗 syslog
- associate Dot11= クライアントの関連付け syslog
- authentication=クライアントの認証成功 syslog
- authfail Dot11=クライアントの認証失敗 syslog
- deauthenticate Dot11=クライアントの認証解除 syslog
- disassociate Dot11=クライアントの関連付け解除 syslog
- excluded Excluded=クライアントの syslog

ステップ 8 コントローラのバッファとコンソールに対するロギング メッセージの重大度レベルを設定するには、次のコマンドを入力します。

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注） 代わりに、*severity_level* パラメータに 0 ～ 7 の数を入力することもできます。

（注） ロギング レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ロギング レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしかログされません。

ステップ 9 次のコマンドを入力して、コントローラ バッファ、コントローラ コンソール、または syslog サーバに対するデバッグ メッセージを保存します。

- **config logging debug buffered {enable | disable}**
- **config logging debug console {enable | disable}**
- **config logging debug syslog {enable | disable}**

デフォルトでは、console コマンドは有効（enable）、buffered コマンドおよび syslog コマンドは無効（disable）です。

ステップ 10 コントローラがメッセージ ログ内にソース ファイルの情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging fileinfo {enable | disable}

デフォルト値はイネーブルです。

ステップ 11 次のコマンドを入力して、プロセス情報をメッセージログに含めるように、またはこの情報を表示しないようにコントローラを設定します。

config logging procinfo {**enable** | **disable**}

デフォルト値は [disabled] です。

ステップ 12 次のコマンドを入力して、トレースバック情報をメッセージログに含めるように、またはこの情報を表示しないようにコントローラを設定します。

config logging traceinfo {enable | disable}

デフォルト値は [disabled] です。

ステップ 13 次のコマンドを入力して、ログ メッセージおよびデバッグ メッセージのタイムスタンプを有効または無効にします。

- **config service timestamps log {datetime | disable}**
- **config service timestamps debug {datetime | disable}**

  値は次のとおりです。

  - **datetime** = 標準の日付と時刻がタイムスタンプとしてメッセージに付加されます。これはデフォルト値です。
  - **disable** = メッセージにタイムスタンプは付加されません。

ステップ 14 次のコマンドを入力して、変更を保存します。

save config

システム ログとメッセージ ログの表示（CLI）

ロギング パラメータとバッファの内容を表示するには、次のコマンドを入力します。

show logging

アクセス ポイント イベント ログの表示

アクセス ポイント イベント ログについて

アクセス ポイントのイベント ログには、すべてのシステム メッセージ（重大度が notifications 以上のもの）が記録されます。イベント ログには最大 1024 行のメッセージを格納できます。1 行あたりの長さは最大 128 文字です。イベント ログがいっぱいになったときは、新しいイベント メッセージを記録するために、最も古いメッセージが削除されます。イベント ログはアクセス ポイント フラッシュ上のファイルに保存されるので、リブートしても消去されません。アクセス ポイント フラッシュへの書き込み回数を最小限にするために、イベント ログの内容がイベント ログ ファイルに書き込まれるのは、通常のリロード時またはクラッシュ時だけとなっています。

アクセス ポイント イベント ログの表示（CLI）

アクセス ポイント イベント ログを表示する、またはコントローラから削除するには、次の CLI コマンドを使用します。

- コントローラに join されたアクセス ポイントのイベント ログ ファイルの内容を表示するには、次のコマンドを入力します。

  show ap eventlog *Cisco_AP*

以下に類似した情報が表示されます。

```
AP event log download has been initiated
Waiting for download to complete

AP event log download completed.
 ========================= AP Event log Contents =====================
*Sep 22 11:44:00.573: %CAPWAP-5-CHANGED: CAPWAP changed state to IMAGE
*Sep 22 11:44:01.514: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to down
*Sep 22 11:44:01.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to down
*Sep 22 11:44:53.539: *** Access point reloading. Reason: NEW IMAGE DOWNLOAD ***
*Mar 1 00:00:39.078: %CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
*Mar 1 00:00:42.142: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:42.151: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:42.158: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:43.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to up
*Mar 1 00:00:43.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to up
*Mar 1 00:00:48.078: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
*Mar 1 00:01:42.144: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:01:48.121: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP
manager IP addresses remain
*Mar 1 00:01:48.122: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
```

- コントローラに join された特定のアクセス ポイントまたはすべてのアクセス ポイントの既存のイベント ログ ファイルを削除して空のイベント ログ ファイルを作成するには、次のコマンドを入力します。

  clear ap-eventlog {**specific** *Cisco_AP* | **all**}

デバッグ ファシリティの使用方法

デバッグ ファシリティにより、コントローラの CPU とやり取りするすべてのパケットを表示できるようになります。受信したパケット、送信したパケット、またはその両方に対して有効にできます。デフォルトでは、デバッグ ファシリティによって受信されたすべてのパケットが表示されます。それらを表示する前に、アクセス コントロール リスト（ACL）を定義してパケットをフィルタリングすることもできます。ACL に渡されないパケットは、表示されずに破棄されます。

各 ACL には、動作（許可、拒否、無効化）、およびパケットの適合に使用する 1 つまたは複数のフィールドが含まれます。デバッグ ファシリティでは、次のレベルおよび値で動作する ACL が提供されます。

- ドライバ ACL
  - NPU のカプセル化の種類

    - ポート

- Ethernet header ACL
    - 宛先アドレス
    - 送信元アドレス
    - イーサネットの種類
    - VLAN ID
- IP header ACL
    - 送信元アドレス
    - 宛先アドレス
    - プロトコル
    - 送信元ポート（該当する場合）
    - 宛先ポート（該当する場合）
- EoIP payload Ethernet header ACL
    - 宛先アドレス
    - 送信元アドレス
    - イーサネットの種類
    - VLAN ID
- EoIP payload IP header ACL
    - 送信元アドレス
    - 宛先アドレス
    - プロトコル
    - 送信元ポート（該当する場合）
    - 宛先ポート（該当する場合）
- CAPWAP payload 802.11 header ACL
    - 宛先アドレス
    - 送信元アドレス
    - BSSID
    - SNAP ヘッダーの種類
- CAPWAP payload IP header ACL

- 送信元アドレス
- 宛先アドレス
- プロトコル
- 送信元ポート（該当する場合）
- 宛先ポート（該当する場合）

各レベルにおいて、複数の ACL を定義できます。パケットと一致する最初の ACL が、選択された ACL となります。

デバッグ ファシリティの設定（CLI）

手順

ステップ 1 デバッグ ファシリティを有効にするには、次のコマンドを入力します。

- **debug packet logging enable** {**rx** | **tx** | **all**} *packet_count display_size*

  値は次のとおりです。

  - **rx** は受信したすべてのパケット、**tx** は送信したすべてのパケット、**all** は受信と送信の両方のパケットを表示します。
  - *packet_count* は、ログするパケットの最大数です。1 ～ 65535 の値をパケット数として入力できます。また、デフォルト値は 25 パケットです。
  - *display_size* は、パケットを印刷する際の表示バイト数です。デフォルトでは、全パケットが表示されます。

    （注） デバッグ ファシリティを無効にするには、**debug packet logging disable** コマンドを入力します。

- **debug packet logging acl driver** *rule_index action npu_encap port*

  値は次のとおりです。

  - *rule_index* の値は、1 ～ 6（両端の値を含む）です。
  - *action* は、permit、deny、または disable です。
  - *npu_encap* では、パケットのフィルタリング方法を定める、NPU のカプセル化の種類を指定します。指定可能な値には、dhcp、dot11-mgmt、dot11-probe、dot1x、eoip-ping、iapp、ip、lwapp、multicast、orphan-from-sta、orphan-to-sta、rbcp、wired-guest などがあります。
  - *port* は、パケットの送受信のための物理ポートです。

- パケットをログする ACL を設定するには、次のコマンドを使用します。

  debug packet logging acl eth *rule_index action dst src type vlan*

  値は次のとおりです。

  - *rule_index* の値は、1 ～ 6（両端の値を含む）です。
  - *action* は、permit、deny、または disable です。
  - *dst* は、宛先の MAC アドレスです。
  - *src* は、送信元の MAC アドレスです。
  - *type* は、2 バイトのタイプ コード（IP の場合は 0x800、ARP の場合は 0x806 など）です。このパラメータには、「ip」（0x800 の代わり）や「arp」（0x806 の代わり）などの一般的な文字列値も使用できます。
  - *vlan* は、2 バイトの VLAN ID です。

- **debug packet logging acl ip** *rule_index action src dst proto src_port dst_port*

  値は次のとおりです。

  - *proto* は、数値、または getprotobyname() で認識される任意の文字列です。サポートされる文字列は、ip、icmp、igmp、ggp、ipencap、st、tcp、egp、pup、udp、hmp、xns-idp、rdp、iso-tp4、xtp、ddp、idpr-cmtp、rspf、vmtp、ospf、ipip、および encap です。
  - *src_port* は 2 バイトの UDP/TCP 送信元ポート（telnet や 23 など）または "any" です。コントローラは getservbyname() で認識される数値または文字列を受け入れます。サポートされる文字列は、tcpmux、echo、discard、systat、daytime、netstat、qotd、msp、chargen、ftp-data、ftp、fsp、ssh、telnet、smtp、time、rlp、nameserver、whois、re-mail-ck、domain、mtp、bootps、bootpc、tftp、gopher、rje、finger、www、link、kerberos、supdup、hostnames、iso-tsap、csnet-ns、3com-tsmux、rtelnet、pop-2、pop-3、sunrpc、auth、sftp、uucp-path、nntp、ntp、netbios-ns、netbios-dgm、netbios-ssn、imap2、snmp、snmp-trap、cmip-man、cmip-agent、xdmcp、nextstep、bgp、prospero、irc、smux、at-rtmp、at-nbp、at-echo、at-zis、qmtp、z3950、ipx、imap3、ulistserv、https、snpp、saft、npmp-local、npmp-gui、および hmmp-ind です。
  - *dst_port* は 2 バイトの UDP/TCP 宛先ポート（telnet や 23 など）または "any" です。コントローラは getservbyname() で認識される数値または文字列を受け入れます。サポートされる文字列は、*src_port* と同じです。

- **debug packet logging acl eoip-eth** *rule_index action dst src type vlan*
- **debug packet logging acl eoip-ip** *rule_index action src dst proto src_port dst_port*
- **debug packet logging acl lwapp-dot11** *rule_index action dst src bssid snap_type*

  値は次のとおりです。

  - *bssid* は、Basic Service Set Identifier（BSSID; 基本サービス セット識別子）です。
  - *snap_type* は、イーサネットの種類です。

- **debug packet logging acl lwapp-ip** *rule_index action src dst proto src_port dst_port*

（注） 設定済みの ACL をすべて削除するには、**debug packet logging acl clear-all** コマンドを入力します。

ステップ 2 デバッグ出力の形式を設定するには、次のコマンドを入力します。

debug packet logging format {**hex2pcap** | **text2pcap**}

デバッグ ファシリティでは、hex2pcap と text2pcap という 2 つの出力形式がサポートされています。IOS によって使用される標準の形式では hex2pcap の使用がサポートされており、HTML フロントエンドを使用してデコードできます。text2pcap オプションは、一連のパケットを同一のコンソール ログ ファイルからデコードできるようにするために用意されています。

図 *2 : Hex2pcap* の出力例

次の図に、hex2pcap の出力例を示します。

```
tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..1n.....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
```

212235

図 *3 : Text2pcap* の出力例

次の図に、text2pcap の出力例を示します。

```
tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..1n.....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@._>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                               NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                               NOPQRS
```

232343

ステップ 3 パケットが表示されない理由を判断するには、次のコマンドを入力します。

debug packet error {**enable** | **disable**}

ステップ 4 パケットのデバッグのステータスを表示するには、次のコマンドを入力します。

show debug packet

以下に類似した情報が表示されます。

```
Status..................................... disabled
Number of packets to display..... 25
Bytes/packet to display..... 0
Packet display format..... text2pcap

Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
```

```
   [6]: disabled
EoIP-IP ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
LWAPP-Dot11 ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
LWAPP-IP ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled?
```