パケット キャプチャ

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 *1 : 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 *2 : 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?
```

無線スニファの設定

無線スニファについて

コントローラには、アクセス ポイントの1つをネットワーク「スニファ」として設定する機能があります。スニファは、特定のチャネル上のパケットをすべてキャプチャして、パケット アナライザ ソフトウェアを実行しているリモート マシンに転送します。これらのパケットには、タイム スタンプ、信号強度、パケット サイズなどの情報が含まれます。スニファを使用すると、ネットワーク アクティビティを監視して記録し、問題を検出できます。

無線スニファの必須条件

無線スニファを実行するには、次のハードウェアとソフトウェアが必要です。

- 専用アクセスポイント：スニファとして設定されたアクセスポイントは、そのネットワーク上で無線アクセス サービスを同時に提供できません。カバレッジの中断を回避するには、既存のワイヤレス ネットワークの一部ではないアクセス ポイントを使用します。
- リモート監視デバイス：アナライザ ソフトウェアを実行できるコンピュータ。
- ソフトウェアおよび関連ファイル、プラグイン、またはアダプタ：アナライザ ソフトウェアによっては、有効にするために特殊なファイルが必要となる場合があります

ワイヤレス スニッフィングの制約事項

- サポートされているサードパーティ製のネットワーク アナライザ ソフトウェア アプリケーションは、次のとおりです。
  - Wildpackets Omnipeek または Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- Wireshark の最新バージョンでは、Analyze モードでパケットをデコードできます。[decode as] を選択し、UDP5555 を PEEKREMOTE としてデコードするように切り替えます。
- アクセス ポイントが Cisco WLC に join されている場合、スニファ モードでアクセス ポイントを使用するためには IP-MAC アドレス バインディングを無効にする必要があります。IP-MAC アドレス バインディングを無効にするには、コントローラ CLI で **config network ip-mac-binding disable** コマンドを入力します。
- アクセス ポイントが Cisco WLC に join されている場合、スニファ モードでアクセス ポイントを使用するためには WLAN 1 を有効にする必要があります。WLAN 1 が無効の場合は、アクセス ポイントはパケットを送信できません。

アクセス ポイントのスニファの設定（GUI）

手順

ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2 スニファとして設定するアクセス ポイントの名前をクリックします。[All APs > Details for] ページが表示されます。

ステップ 3 [AP Mode] ドロップダウン リストから [Sniffer] を選択します。

ステップ 4 [Apply] をクリックします。

ステップ 5 アクセス ポイントをリブートするプロンプトが表示されたら、[OK] をクリックします。

ステップ 6 [Wireless] > [Access Points] > [Radios] > [802.11a/n]（または [802.11b/g/n]）を選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます。

ステップ 7 カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて [Configure] を選択します。[802.11a/n/ac]（または 802.11b/g/n）Cisco APs] > [Configure] ページが表示されます。

ステップ 8 [Sniff] チェックボックスをオンにして、このアクセス ポイントのスニファを有効にします。オンにしなければ、スニファは無効になります。デフォルトではオフになっています。

ステップ 9 ステップ 8 でスニファを有効にした場合は、次の手順に従ってください。

a) [Channel] ドロップダウン リストから、アクセス ポイントがパケットに対してスニファするチャネルを選択します。

b) [Server IP Address] テキスト ボックスに、Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスを入力します。

ステップ 10 [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

アクセス ポイントのスニファの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、アクセス ポイントをスニファとして設定します。

config ap mode sniffer *Cisco_AP*

Cisco_AP はスニファとして設定されるアクセス ポイントです。

ステップ 2 アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。アクセス ポイントはスニファ モードでリブートします。

ステップ 3 次のコマンドを入力して、アクセス ポイントでスニファを有効にします。

config ap sniff {802.11a | 802.11b} enable *channel server_IP_address Cisco_AP*

値は次のとおりです。

- *channel* はアクセス ポイントがパケットに対してスニファする無線チャンネルです。デフォルト値は 36（802.11a/n/ac）と 1（802.11b/g/n）です。
- *server_IP_address* は Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスです。
- *Cisco_AP* はスニファとして設定されるアクセス ポイントです。

（注） アクセス ポイントでスニファを無効にするには、**config ap sniff** {**802.11a** | **802.11b**} **disable** *Cisco_AP* コマンドを入力します。

ステップ 4 次のコマンドを入力して、変更を保存します。

save config

ステップ 5 次のコマンドを入力して、アクセス ポイントのスニファの設定を表示します。

show ap config {**802.11a** | **802.11b**} *Cisco_AP*