CHAPTER 7

ポートおよびポート プロファイル

この章では、ポートに関する問題を識別して解決する方法について説明します。この章の内容は次のとおりです。

概要

スイッチで 1 つのデータ リンクから別のデータ リンクへのフレーム リレーを行うには、フレームが送受信されるインターフェイスの特性を定義する必要があります。設定されるインターフェイスは、イーサネット（物理）インターフェイス、仮想イーサネット インターフェイス（mgmt0）、および管理インターフェイス（mgmt0）です。

各インターフェイスには、次の設定があります。

- 管理設定

  管理設定は、修正を加えない限り変更されません。この設定には、管理モードで設定できる属性があります。

- 動作状態

  指定された属性（インターフェイス速度など）の動作状態。この状態は読み取り専用なので、変更できません。インターフェイスがダウンしているときは、一部の値（動作速度など）が有効にならない場合があります。

ポート モード、管理状態、および動作状態の詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*』を参照してください。

ポート インターフェイスの設定に関する注意事項

ポート インターフェイスを設定する際には、次の注意事項に従ってください。

- 「モジュールの状態の確認」（P.7-2）の手順に従って、モジュールがアクティブであることを確認する。

モジュールの状態の確認

次の手順に従って、モジュールの状態を確認します。

はじめる前に

- コマンドの出力に、モジュールが「OK」（アクティブ）と表示される必要があります。

手順の詳細

ステップ 1　EXEC モードで、次のコマンドを入力します。

show module *module-number*

例：

```
n1000v# show mod 3
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------- ------------------ ------------
3    248    Virtual Ethernet Module                              ok

Mod  Sw              Hw
---  --------------  ------
3    NA              0.0

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------
3    192.168.48.20    496e48fa-ee6c-d952-af5b-001517136344  frodo
```

診断チェックリスト

次のチェックリストを使用して、ポート インターフェイス アクティビティの診断を開始します。

チェックリスト	√
show svs connections コマンドを使用して、Virtual Supervisor Module（VSM; 仮想スーパーバイザ モジュール）が vCenter Server に接続されていることを確認します。	
vCenter Server に接続されている vSphere Client で物理 Network Interface Card（NIC; ネットワーク インターフェイス カード）と仮想 NIC を確認して、それぞれの NIC に適切なポート プロファイルが割り当てられていることを確認します。	
show interface brief コマンドを使用してポートが作成されていることを確認します。	
「ポート状態の表示」（P.7-4）の手順に従って、インターフェイスの状態を確認します。ポート状態の詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*』を参照してください。	

ポートのトラブルシューティングには、次のコマンドを使用します。

- **show interface status**
- **show interfaces capabilities**
- **show system internal ethpm errors**
- **show system internal ethpm event-history**
- **show system internal ethpm info**
- **show system internal ethpm mem-stats**
- **show system internal ethpm msgs**
- **show system internal vim errors**
- **show system internal vim event-history**
- **show system internal vim info**
- **show system internal vim mem-stats**
- **show system internal vim msgs**

ポート状態の表示

次の手順に従って、ポート状態を表示します。

はじめる前に

- コマンドの出力には、次の情報が表示されます。
  - 管理状態
  - 速度
  - トランク VLAN のステータス
  - 送受信されたフレームの数
  - 伝送エラー（破棄、エラー、Cyclic Redundancy Check（CRC; 巡回冗長検査）、および不正なフレームなど）

手順の詳細

ステップ 1　EXEC モードで、次のコマンドを入力します。

show interface ethernet *slot-number*

例：

```
n1000v# show int eth3/2
Ethernet3/2 is up
  Hardware: Ethernet, address: 0050.5653.6345 (bia 0050.5653.6345)
  MTU 1500 bytes, BW -598629368 Kbit, DLY 10 usec,
     reliability 0/255, txload 0/255, rxload 0/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned off
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Switchport monitor is off
    Rx
    18775 Input Packets 10910 Unicast Packets
    862 Multicast Packets 7003 Broadcast Packets
    2165184 Bytes
    Tx
    6411 Output Packets 6188 Unicast Packets
    216 Multicast Packets 7 Broadcast Packets 58 Flood Packets
    1081277 Bytes
    1000 Input Packet Drops 0 Output Packet Drops
    1 interface resets
n1000v#
```

ポート カウンタの使用

カウンタを使用して受信フレーム数と送信フレーム数の有意差を表示することにより、同期の問題を識別できます。

はじめる前に

- 最初に、カウンタをクリアしてベースラインを作成します。

  長期間にわたってアクティブになっていたポートの場合、カウンタに格納されている値は意味を持たないことがあります。カウンタをクリアすることにより、現時点での実際のリンクの動作をより正確に把握できます。

手順の詳細

ステップ 1　EXEC モードで、次のコマンドを入力して、インターフェイスのカウンタをゼロに設定します。

clear counters interface ethernet *slot-number*

例：

```
n1000v# clear counters interface eth 2/45
n1000v#
```

ステップ 2　次のコマンドを入力して、ポート カウンタを表示します。

show interface ethernet *slot number* **counters**

例：

```
n1000v# show interface eth3/2 counters

--------------------------------------------------------------------------------
Port                 InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Eth3/2              2224326         11226           885           7191

--------------------------------------------------------------------------------
Port                OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
Eth3/2              1112171          6368           220              7
```

ポート インターフェイスの現象および解決方法

ここでは、次の現象に対して考えられる原因および解決方法について説明します。

- 「インターフェイスをイネーブルにできない」（P.7-6）
- 「ポートがリンク障害または接続されていない状態のままになっている」（P.7-6）
- 「リンク フラッピング」（P.7-6）
- 「ポートが errDisabled 状態になっている」（P.7-7）

インターフェイスをイネーブルにできない

現象	考えられる原因	解決方法
インターフェイスをイネーブルにできない	レイヤ 2 ポートがアクセス VLAN に関連付けられていない、または VLAN が一時停止状態にある。	**show interface brief** CLI コマンドを使用して、VLAN 内でインターフェイスが設定されているかどうかを調べます。**show vlan brief** CLI コマンドを使用して、VLAN のステータスを調べます。VLAN コンフィギュレーション モードで **state active** CLI コマンドを使用して、VLAN の状態をアクティブに設定します。

ポートがリンク障害または接続されていない状態のままになっている

現象	考えられる原因	解決方法
ポートが link-failure 状態のままになっている	ポート接続が不良である。	**show system internal ethpm info** CLI コマンドを使用して、ポートのステータスが「link-failure」になっていることを確認します。 **shut** コマンド、**no shut** コマンドの順に入力して、ポートをいったんディセーブルにしてからイネーブルにします。これで問題が解決しない場合は、同じモジュールの別のポートまたは他のモジュールのポートに接続を移動してみます。
	リンクが初期化状態で停止している。または、リンクがポイントツーポイント状態になっている。	**show logging** CLI コマンドを使用して、「`Link Failure, Not Connected`」システム メッセージが出力されるかどうかを調べます。 **shut** CLI コマンド、**no shut** コマンドの順に入力して、ポートをいったんディセーブルにしてからイネーブルにします。これで問題が解決しない場合は、同じモジュールの別のポートまたは他のモジュールのポートに接続を移動してみます。
	—	上記の手順を VSM で実行しても問題を解決できない場合は、**vss-support** コマンドを使用して ESX 側の NIC 設定を収集します。

リンク フラッピング

ここでは、次の内容について説明します。

- 「リンク フラッピング サイクルについて」（P.7-7）
- 「トラブルシューティングの前提条件」（P.7-7）
- 「現象、原因、および解決方法」（P.7-7）

リンク フラッピング サイクルについて

ポートでフラッピングが発生すると、ポート状態が次の順序で変化し、一巡すると、最初の状態に戻って繰り返します。

1. Initializing：リンクを初期化しています。
2. Offline：ポートはオフライン状態です。
3. Link failure or not connected：物理レイヤ リンクが動作不能で、アクティブなデバイス接続がありません。

トラブルシューティングの前提条件

予期しないリンク フラッピングのトラブルシューティング時には、次の情報を把握することが重要です。

- リンク フラッピングを発生させたユーザ
- リンク ダウンの実際の原因

現象、原因、および解決方法

現象	考えられる原因	解決方法
予期しないリンク フラッピングが発生する	ビット レートがしきい値を超えたために、ポートが errDisabled 状態になっている。	Device Manager でポートを右クリックし、[disable] を選択してから [enable] を選択します。または、**shut CLI** コマンド、**no shut** コマンドの順に入力して、ポートを通常の状態に戻します。
	スイッチの問題により、エンド デバイスでリンク フラップ動作が発生している。次のような原因が考えられる。 • ハードウェア障害または断続的なハードウェア エラーにより、スイッチでパケットがドロップされた。 • ソフトウェア エラーによってパケットがドロップされた。 • 制御フレームが誤ってデバイスに送信された。	MAC ドライバによって示されるリンク フラップの原因を確認します。エンド デバイス上のデバッグ機能を使用して、問題のトラブルシューティングを行います。外部デバイスでは、エラーが発生すると、リンクの再初期化が選択されることがあります。そのような場合、リンクを再初期化する具体的な方法はデバイスによって異なります。
	リンク フラッピングは、ESX のエラー、またはアップストリーム スイッチのリンク フラッピングによって発生する可能性がある。	

ポートが errDisabled 状態になっている

ここでは、次の内容について説明します。

- 「errDisabled のポート状態について」（P.7-8）
- 「errDisable 状態の確認」（P.7-8）
- 「errDisable 状態の確認」（P.7-8）

errDisabled のポート状態について

errDisabled 状態とは、スイッチがポートの問題を検出して、そのポートをディセーブルにしたことを示します。この状態は、ポート フラッピングまたは大量の不良フレーム（CRC エラー）によって発生し、メディアに問題があることを示している可能性があります。

errDisable 状態の確認

CLI を使用して errDisable 状態を解決するには、次の手順に従います。

ステップ 1　**show interface** コマンドを使用して、スイッチが問題を検出してポートをディセーブルにしたことを確認します。ケーブルを調べます。

```
n1000v# show interface e1/14
e1/7 is down (errDisabled)
```

ステップ 2　**show port internal event-history interface** コマンドを使用して、ポートの内部状態の遷移に関する情報を表示します。この例では、機能の不一致（「CAP MISMATCH」）が原因で、ポート e1/7 が errDisabled 状態になっています。このイベントをどのように解釈するかがわからない場合は、他のコマンドを使用して詳細な情報を参照できます。

```
n1000v# show port internal event-history interface e1/7
>>>>FSM: <e1/7> has 86 logged transitions<<<<<
1) FSM:<e1/7> Transition at 647054 usecs after Tue Jan  1 22:44..
    Previous state: [PI_FSM_ST_IF_NOT_INIT]
    Triggered event: [PI_FSM_EV_MODULE_INIT_DONE]
    Next state: [PI_FSM_ST_IF_INIT_EVAL]
2) FSM:<e1/7> Transition at 647114 usecs after Tue Jan  1 22:43..
    Previous state: [PI_FSM_ST_IF_INIT_EVAL]
    Triggered event: [PI_FSM_EV_IE_ERR_DISABLED_CAP_MISMATCH]
    Next state: [PI_FSM_ST_IF_DOWN_STATE]
```

ステップ 3　**show logging logfile** コマンドを使用してスイッチのログ ファイルを表示し、ポート状態の変化を確認します。次の例に示すエラーは、ある管理者がポート e1/7 をポート チャネル 7 に追加しようとしたときに記録されたものです。このポートがポート チャネル 7 とまったく同じように設定されていなかったため、試行が失敗しました。

```
n1000v# show logging logfile
 . . .
Jan  4 06:54:04 switch %PORT_CHANNEL-5-CREATED: port-channel 7 created
Jan  4 06:54:24 switch %PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-channel 7
is down (No operational members)
Jan  4 06:54:40 switch %PORT_CHANNEL-5-PORT_ADDED: e1/8 added to port-channel 7
Jan  4 06:54:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: Interface e1/7 is down (Admnistratively
down)
Jan  4 06:54:59 switch %PORT_CHANNEL-3-COMPAT_CHECK_FAILURE: speed is not compatible
Jan 4 06:55:56 switch%PORT_CHANNEL-5-PORT_ADDED: e1/7 added to port-channel 7
```

ポート セキュリティ

ポート セキュリティ機能を使用すると、ポートにアクセスできる MAC アドレスを制限および識別することによってポートをセキュリティで保護できます。セキュア MAC は、手動で設定するか、ダイナミックに学習されます。

セキュリティ違反には、次の 2 種類があります。

- アドレス カウント超過違反
- MAC 移動違反

ポート セキュリティは、次のポート タイプでサポートされます。

- 仮想イーサネット アクセス ポート
- 仮想イーサネットトランク ポート

仮想イーサネット SPAN 宛先ポートでは、ポート セキュリティはサポートされません。また、独立型イーサネット インターフェイスやポート チャネルのメンバー上でも、ポート セキュリティはサポートされません。

ポート セキュリティに関する問題のトラブルシューティング

ここでは、インターフェイス上でポート セキュリティがイネーブルになっているときに発生する、次の接続に関する問題をトラブルシューティングする方法について説明します。

- ポート セキュリティがイネーブルになっているときに VM から ping できない
- ポート セキュリティがイネーブルになっているポートが errDisabled 状態になっている

ポート セキュリティがイネーブルになっているときに VM から ping できない

ポート セキュリティがイネーブルになっているときに Virtual Machine（VM; 仮想マシン）から ping を実行できない場合は、次の手順に従います。

ステップ 1　**module vem 3 execute vemcmd show portsec stats** コマンドを入力して、ポートに適用されている実際のポート セキュリティ設定を表示します。

構文：**module vem** *vem number* **execute vemcmd show portsec stats**

```
n1000V#module vem 3 execute vemcmd show portsec stats
  LTL   if_index  cp-cnt  Max         Aging   Aging     DSM  Sticky   VM
                          Secure      Time    Type      Bit  Enabled  Name
                          Addresses
   47   1b020000       0          1       0   Absolute  Clr       No  VM-Pri.eth1
```

この出力は、LTL 47 が VM-Pri 仮想マシンのネットワーク アダプタ 1 に接続されているインターフェイス上でポート セキュリティがイネーブルになっていることを示します。

また、この出力は他のセキュリティ設定属性も示しており、最大セキュア アドレス数は 1、エージング タイプは Absolute、エージング タイムは 0 秒（つまり、エージングはディセーブル）、Sticky MAC はディセーブルになっています。

注意　Drop on Source Miss（DSM; 送信元の失敗時に廃棄）を設定すると、このポートは新しい MAC アドレスを学習できません。

DSM ビットをクリアするには、VSM で **no port-security stop learning** コマンドを入力します。

```
n1000V# no port-security stop learning
```

DSM ビットを設定しない場合は、ステップ 2 に進みます。

ステップ 2　VM を含む ESX ホストにログインし、**module vem 3 execute vemcmd show portsec macs all** コマンドを入力して、その VEM のすべてのセキュア MAC を表示します。

```
~ #module vem 3 execute vemcmd show portsec macs all
VLAN 65's Secure MAC list:
     cp MAC 08:66:5c:99:72:f2  LTL    48  timeout       960
```

「cp」は、現在処理中であることを意味します。つまり、このパケットは、VSM 上で実行されているポート セキュリティ プロセスによって確認されていません。

この確認通知は、インバンド チャネルを通じて送信されます。

確認通知はインバンド チャネルを通じて送信されるため、インバンド VLAN は、アップストリーム スイッチの対応するポートと同様、VEM のいずれかのアップリンク ポート上に存在する必要があります。

ステップ 3　**show svs domain** コマンドを使用して、パケット VLAN（インバンド VLAN）を調べます。

```
n1000v(config-port-prof)# show svs domain
SVS domain config:
  Domain id:    559
  Control vlan: 3002
  Packet vlan:  3003
  L2/L3 Aipc mode: L2
  L2/L3 Aipc interface: mgmt0
  Status: Config push to VC successful.
```

この出力では、パケット VLAN は 69 です。

ステップ 4　VEM のいずれかのアップリンク ポート上でパケット VLAN が許可されていることを確認します。

1 つのアップリンクがポート プロファイル アップリンク プロファイルにバインドされているとします。**show port-profile na uplink-all** コマンドを次のように入力します。

```
n1000v# show port-profile na uplink-all
port-profile uplink-all
description:
type: vethernet
status: enabled
capability l3control: no
pinning control-vlan: -
pinning packet-vlan: -
system vlans: 69-69
port-group: uplink-all
max ports:
inherit: port-profile xyz
config attributes:
 switchport mode trunk
 switchport access vlan 1
 switchport trunk allowed vlan 1, 68-69,231-233
 channel-group auto mode on sub-group cdp
 no shutdown
evaluated config attributes:
 switchport mode trunk
 switchport trunk allowed vlan 1,68-69,231-233
 channel-group auto mode on sub-group cdp
 no shutdown
assigned interfaces:
  Ethernet3/2
```

この出力が示すように、アップリンク プロファイルはイーサネット 3/2 に割り当てられ、このポート上でインバンド VLAN（69）が許可されています。許可されていない場合は、許可される VLAN のリストにパケット VLAN（69）を追加します。

ステップ 5　**show cdp neighbors** コマンドを入力して、イーサネット インターフェイス 3/2 に接続されているアップストリームのネイバーを調べます。

```
n1000V#show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
swordfish-6k-2         Eth3/2        149    R S I       WS-C6506-E    Gig1/38
```

この出力は、イーサネット インターフェイス 3/2 がギガビット インターフェイス 1/38 上のスイッチ n1000v-6k-2 に接続されていることを示します。

n1000v-6k-2 にログインし、ポート上でパケット VLAN が許可されていることを確認します。

```
n1000v-6k-2#show running-config interface gigabitEthernet 1/38
Building configuration...

Current configuration : 161 bytes
!
interface GigabitEthernet1/38
 description sfish-srvr-100:vmnic1
 switchport
 switchport trunk allowed vlan 1,60-69,231-233
 switchport mode trunk
end
```

この出力は、ポート上でパケット VLAN 69 が許可されていることを示します。許可されていない場合は、許可される VLAN のリストにパケット VLAN を追加します。

ポート セキュリティがイネーブルになっているポートが errDisabled 状態になっている

errDisabled 状態とは、スイッチがポートの問題を検出して、そのポートをディセーブルにしたことを示します。ポート セキュリティは、次の理由でポートをディセーブルにするエラーに対して有効です。

- アドレス カウント超過違反
- MAC 移動違反

アドレス カウント超過違反

この問題は、設定した最大セキュア アドレス数を超えるアドレスがポート上で検出されると発生します。違反に対するデフォルト アクションでは、エラーによってポートがディセーブルになります。この問題を見つける 1 つの方法は、**show logging** コマンドの出力に対して、検索パターン「PORT-SECURITY-2-」で **grep** コマンドを実行することです。

```
n1000v#show port-security address interface vethernet 1
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

------------------------------------------------------------------------
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining age
                                                               (mins)
----    -----------             ------           -----     ---------------
  65    0050.56B7.7DE2        DYNAMIC        Vethernet1        0
========================================================================
```

この出力は、veth1 上で MAC 0050.56B7.7DE2 が保護されていることを示します。

```
n1000V#show port-security
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

------------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
------------------------------------------------------------------------------
Vethernet1            1              0              0              Shutdown
==============================================================================
```

最大セキュア アドレス数は 1 です。

仮想イーサネット 1 上に別の MAC アドレス E276.DECF.7DE2 が出現します。これにより、ポートは errDisabled 状態になります。

```
n1000v# show logging | inc "PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN"

2008 Dec 20 21:33:44 N1KV %PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN:
Port Vethernet1 moved to SHUTDOWN state as host E276.DECF.7DE2 is trying to access the
port in vlan 65
```

MAC 移動違反

MAC 移動違反は、特定のポート（たとえば、ポート A）上ですでに保護されている MAC アドレスが別のセキュア ポート（たとえば、ポート B）上で検出されると発生します。

```
n1000v#show port-security address interface vethernet 1
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

------------------------------------------------------------------------
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining age
                                                               (mins)
----    -----------             ------           -----      ---------------
  65    0050.56B7.7DE2        DYNAMIC        Vethernet1         0
========================================================================
```

この出力は、veth1 上で MAC 0050.56B7.7DE2 が保護されていることを示します。

```
n1000v#show port-security
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

-------------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
-------------------------------------------------------------------------------
Vethernet1            1             0              0              Shutdown
===============================================================================
```

この出力は、最大セキュア アドレス数が 1 であることを示します。

仮想イーサネット 1 上に MAC アドレス E276.DECF.7DE2 が出現します。これにより、ポートは errDisabled 状態になります。

```
n1000v# show logging | inc "PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN"

2008 Dec 20 21:33:44 N1KV
%PORT-SECURITY-2-ETH_PORT_SEC_SECURITY_VIOLATION_MAX_MAC_VLAN: Port
Vethernet1 moved to SHUTDOWN state as host E276.DECF.7DE2 is trying to access the port in vlan 65
```

ポートセキュリティに関する制限および制約事項

ポート セキュリティに関する問題のトラブルシューティング時には、次の注意事項に従ってください。

- ダイナミックなセキュア MAC アドレスは、**clear mac address-table** コマンドを使用して消去できない。代わりに、**clear port-security** コマンドを使用する。
- 同じ VLAN 上にスタティックな MAC アドレスが設定されている場合は、VLAN の Veth 上でポート セキュリティをイネーブルにすることができない。VLAN の Veth 上でポート セキュリティをイネーブルにするには、任意のインターフェイスの VLAN 上に存在するスタティックな MAC アドレスを削除する必要がある。
- 違反の制限アクションはサポートされない。シャットダウン違反モードと保護違反モードのみ、ポート セキュリティ違反アクションとして設定できる。

ポート セキュリティのデバッグ出力の収集

ポート セキュリティのトラブルシューティングには、次のコマンドを使用します。

- **show port-security**
- **show port-security interface veth**
- **show port -security address**

VSM では、次のコマンドを使用して情報を収集し、ポート セキュリティのトラブルシューティングを行います。

- **show system internal port-security msgs**
- **show system internal port-security errors**
- **show system internal l2fm msgs**
- **show system internal l2fm errors**
- **show system internal l2fm info detail**
- **show system internal pktmgr interface brief**
- **show system internal pktmgr client detail**

現象、原因、および解決方法

現象	考えられる原因	解決方法
ポート セキュリティがイネーブルになっているインターフェイス上で、VM からの ping が失敗する	—	VM からの最初のパケットが VSM に送信されたことを確認します。 ESX ホストのアップリンク ポートおよびアップリンク スイッチのポートがインバンド VLAN を伝送していることを確認します。 CPVA をホスティングしている ESX ポート（およびアップリンク スイッチの対応するポート）がインバンド VLAN を伝送していることを確認します。 パケット マネージャで、Veth インターフェイスの状態が UP であることを確認します。UP でない場合は、Veth インターフェイスで、**shutdown** コマンド、**no shutdown** コマンドの順に入力します。

ポート プロファイル

ポート プロファイルを使用してインターフェイスを設定します。1 つのポート プロファイルを複数のインターフェイスを割り当てることで、すべてのインターフェイスを同じ設定にすることができます。ポート プロファイルに対する変更は、そのポート プロファイルに割り当てられているすべてのインターフェイスの設定に自動的に伝播されます。

VMware vCenter Server では、ポート プロファイルはポート グループとして表されます。vCenter Server では、仮想イーサネット インターフェイスやイーサネット インターフェイスは、次の目的でポート プロファイルに割り当てられます。

- ポリシーによってポート設定を定義する。
- 単一ポリシーを多数のポートに適用する。
- 仮想イーサネット ポートとイーサネット ポートをサポートする。

アップリンクとして設定されているポート プロファイルは、サーバ管理者によって物理ポート（vmnic または pnic）に割り当てられます。アップリンクとして設定されていないポート プロファイルは、VM 仮想ポートに割り当てられます。

（注） 手動インターフェイス設定でポート プロファイルの設定を上書きすることもできますが、この方法は推奨できません。手動インターフェイス設定は、たとえば、すばやく変更をテストする場合や、継承されたポート プロファイルを変更する必要なくポートをディセーブルにすることを許可する場合だけ使用します。

ポート プロファイルの割り当ての詳細については、VMware のマニュアルを参照してください。

プロファイルが正しく割り当てられていることを確認するには、次の show コマンドを使用します。

- **show port-profile usage**
- **show running-config interface** *interface-id*

show running-config interface *interface-id* コマンドの出力には、継承されたポート プロファイルであることを示す `inherit port-profile MyProfile` などの設定行が表示されます。

（注） 継承されたポート プロファイルは、CLI を使用して変更したり、インターフェイスから削除したりできません。このような操作は、vCenter Server を使用する場合だけ実行できます。

（注） ポートがホストに接続されている場合、継承されたポート プロファイルは自動設定されます。これは、システム管理者によって割り当てられた VMware ポート グループを作成元のポート プロファイルと比較することによって行います。

ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*』を参照してください。

ポート プロファイルのトラブルシューティング コマンド

ポート プロファイルの詳細なログを収集するには、デバッグ ログを収集する、次のコマンドを実行します。

- **debug port-profile trace**
- **debug port-profile error**
- **debug port-profile all**

デバッグ ログをイネーブルにしたら、ポート プロファイルの操作を再実行して、出力をログ ファイルにキャプチャします。

ポート プロファイルのトラブルシューティングには、次のコマンドを使用します。

- **show port-profile**

```
n1000v# show port-profile
port-profile UpLinkProfile1
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on mac-pinning
  evaluated config attributes:
    channel-group auto mode on mac-pinning
  assigned interfaces:
port-profile UpLinkProfile2
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group cdp
  evaluated config attributes:
    channel-group auto mode on sub-group cdp
  assigned interfaces:
port-profile UpLinkProfile3
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group manual
  evaluated config attributes:
    channel-group auto mode on sub-group manual
  assigned interfaces:n1000v#
```

- **show port-profile expand-interface**

```
n1000v# show port-profile expand-interface
```

```
port-profile uplink1
Ethernet3/2
    switchport mode trunk
    switchport trunk allowed vlan 1,110-119
    no shutdown
Ethernet4/2
    switchport mode trunk
    switchport trunk allowed vlan 1,110-119
    no shutdown

port-profile data
Vethernet1
    switchport mode access
    switchport access vlan 118
    no shutdown
n1000v#
```

- **show port-profile usage**

```
n1000v# show port-profile usage

------------------------------------------------------------------------------
Port Profile               Port        Adapter        Owner
------------------------------------------------------------------------------
uplink1                    Eth3/2      vmnic1         172.23.232.57
                          Eth4/2      vmnic1         172.23.232.58
data                       Veth1       Net Adapter 1  ubuntu-2
n1000v#
```

- **show port-profile internal info**

```
n1000v# show port-profile internal info
port-profile Unused_Or_Quarantine_Uplink
  ppid: 00000001
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000002
  description: "Port-group created for Nexus1000V internal usage. Do not use."
  alias_id: Unused_Or_Quarantine_Uplink (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1060
    flags: 00000000
  alias name: dvportgroup-1060 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 0
port-profile Unused_Or_Quarantine_Veth
  ppid: 00000002
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000000
  description: "Port-group created for Nexus1000V internal usage. Do not use."
  alias_id: Unused_Or_Quarantine_Veth (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1061
    flags: 00000000
  alias name: dvportgroup-1061 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
```

```
  num_active_ifs: 0
port-profile uplink1
  ppid: 00000003
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000003
  description: ""
  alias_id: uplink1 (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1062
    flags: 00000000
  alias name: dvportgroup-1062 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 1
  Ethernet3/2:
    flags: 00000000
    is_active: true
    is_user_configured: false
    bind_count: 1
    is_bound_by_eth_attach: 1
port-profile data
  ppid: 00000005
  flags: 00000000
  fsm_state: PPM_PROFILE_FSM_ST_CREATED
  state: enabled
  capability: 00000000
  description: ""
  alias_id: data (type=1)
  num_aliases: 1
  alias (type=2):
    name: dvportgroup-1064
    flags: 00000000
  alias name: dvportgroup-1064 type: 2 (pss)
  parent port-profile: none
  num_child_profiles: 0
  num_active_ifs: 0
vms info flag: 00000001
n1000v#
```

- **show port-profile internal event-history msgs**

```
n1000v# show port-profile internal event-history msgs
1) Event:E_MTS_RX, length:60, at 553112 usecs after Thu May 14 00:28:52 2009
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X0028B018, Ret:SUCCESS
    Src:0x00000101/3929, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x0028B018, Sync:NONE, Payloadsize:212
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 31 37

2) Event:E_MTS_RX, length:60, at 472402 usecs after Thu May 14 00:28:48 2009
    [REQ] Opc:MTS_OPC_SDWRAP_DEBUG_DUMP(1530), Id:0X0028AF64, Ret:SUCCESS
    Src:0x00000101/3928, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x0028AF64, Sync:NONE, Payloadsize:212
    Payload:
    0x0000:  01 00 2f 74 6d 70 2f 64 62 67 64 75 6d 70 31 37

3) Event:E_MTS_RX, length:60, at 897349 usecs after Thu May 14 00:24:59 2009
    [REQ] Opc:MTS_OPC_VSH_CMD_TLV(7679), Id:0X00289DB3, Ret:SUCCESS
    Src:0x00000101/3899, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00289DB3, Sync:NONE, Payloadsize:228
    Payload:
```

```
    0x0000:  04 03 02 01 e4 00 00 00 00 00 00 00 00 00 00 00

4) Event:E_MTS_RX, length:60, at 171002 usecs after Thu May 14 00:19:27 2009
    [REQ] Opc:MTS_OPC_VSH_CMD_TLV(7679), Id:0X00288A62, Ret:SUCCESS
    Src:0x00000101/3899, Dst:0x00000101/429, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x00288A62, Sync:NONE, Payloadsize:220
    Payload:
    0x0000:  04 03 02 01 dc 00 00 00 00 00 00 00 00 00 00 00
```

- **show port-profile internal event-history port-profile** *profile-name*

```
n1000v# show port-profile internal event-history port-profile data

>>>>FSM: <port-profile/5> has 6 logged transitions<<<<<

1) FSM:<port-profile/5> Transition at 212488 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_NOT_EXISTENT]
    Triggered event: [PPM_PROFILE_FSM_EV_INIT]
    Next state: [PPM_PROFILE_FSM_ST_CREATED]

2) FSM:<port-profile/5> Transition at 212494 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_CREATED]
    Triggered event: [PPM_PROFILE_FSM_EV_CFG_CHANGED]
    Next state: [PPM_PROFILE_FSM_ST_UPDATING_EVAL_CFG]

3) FSM:<port-profile/5> Transition at 212516 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_UPDATING_EVAL_CFG]
    Triggered event: [PPM_PROFILE_FSM_EV_EVAL_CFG_CHANGED]
    Next state: [PPM_PROFILE_FSM_ST_MSP_HANDSHAKE_CFG_CHANGE]

4) FSM:<port-profile/5> Transition at 212535 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_MSP_HANDSHAKE_CFG_CHANGE]
    Triggered event: [PPM_PROFILE_FSM_EV_MSP_HANDSHAKE_FAIL]
    Next state: [PPM_PROFILE_FSM_ST_UPDATING_CLIENTS]

5) FSM:<port-profile/5> Transition at 212542 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_UPDATING_CLIENTS]
    Triggered event: [PPM_PROFILE_FSM_EV_UPDATE_DONE]
    Next state: [PPM_PROFILE_FSM_ST_WAIT_FOR_CHILD]

6) FSM:<port-profile/5> Transition at 213668 usecs after Mon May 11 19:45:02 2009
    Previous state: [PPM_PROFILE_FSM_ST_WAIT_FOR_CHILD]
    Triggered event: [PPM_PROFILE_FSM_EV_CHILD_PROFILE_DONE]
    Next state: [PPM_PROFILE_FSM_ST_CREATED]
```

システム ポート プロファイル

システム ポート プロファイルは、VSM と VEM が相互に通信できるように、事前に設定しておく必要がある特別なポート プロファイルです。システム ポート プロファイルは、コントロール VLAN とパケット VLAN の ID を、vCenter Server 経由で VSM から VEM に伝送するために使用されます。

システム ポート プロファイルの設定時には、次の注意事項に従ってください。

- トランク ポートの場合、システム VLAN のリストは、許可される VLAN のリストの一部である必要がある。
- アクセス ポートの場合、アクセス VLAN と同じシステム VLAN が 1 つ存在する必要がある。
- **no system vlan** コマンドは、プロファイルを使用しているインターフェイスが存在しない場合だけ実行する。

- システム プロファイルが 1 つ以上のインターフェイスによって使用されている場合、システム VLAN のリストに VLAN を追加することはできるが、リストから VLAN を削除することはできない。
- プロファイルにシステム VLAN が含まれる場合は、そのプロファイルを使用しているインターフェイスが存在しない場合だけ、**no port-profile** コマンド、**no vmware port-group** コマンド、および **no state enabled** コマンドを実行できる。
- ポート プロファイルの最大数は 128 である。

ポート プロファイルの現象および解決方法

現象	考えられる原因	解決方法
vCenter Server 上にポート グループが表示されない、または「Warning: Operation succeeded locally but update failed on vCenter server. Please check if you are connected to vCenter Server.」というメッセージが表示される。	—	**show svs connections** コマンドを入力して、vCenter Server への接続がアクティブになっていることを確認します。スイッチの出力に「Enabled」と「Connected」が表示されている必要があります。 **show svs domain** コマンドを実行して、Status が「successful」と表示されていることを確認します。 ポート プロファイルに対して次のコマンドが指定されていることも確認します。 • **vmware port-group** • **state enabled**
ポートの設定がインターフェイスに適用されない。	—	**show port-profile usage** コマンドを実行して、インターフェイスを表示します。 **show run** コマンドおよび **show port-profile expand-interface** コマンドを使用して、インターフェイス レベル設定でポート プロファイルの設定が上書きされていないことを確認します。
イーサネット インターフェイスまたは Veth インターフェイスが管理上のダウン状態になっている。	インターフェイスがいずれかの検疫ポート プロファイルを継承しようとしている。**show port-profile usage** コマンドを実行して、状況を確認する。	vnic または pnic を非検疫ポート グループに再割り当てし、Veth インターフェイスまたはイーサネット インターフェイスが起動し、トラフィックを転送できるようにします。このアクションでは、vCenter Server 上のポート グループを変更する必要があります。

VSM から vCenter Server へのポート プロファイルの転送

VSM から vCenter Server へのポート プロファイル転送時には、次の注意事項に従ってください。

- Uplink Port Profile（UPP; アップリンク ポート プロファイル）に次の必須属性が含まれることを確認します。
  - capability uplink
  - system vlans（システム ポート プロファイルの場合に設定）

（注）　トランク モードを構成している場合、特権プロファイルには、必ずプロファイル内で VLAN を明示的に許可してください。このタイプの設定には、**switchport trunk allowed vlan** *your-vlan -list* コマンドを入力します。

  - Vmware port group
  - switchport trunk/access
  - no shutdown
  - state enabled
- ポート プロファイル内ではすべての VLAN を明示的に作成してください。