Cisco Nexus 5000 トラブルシューティング ガイド

Cisco Nexus 5000 Troubleshooting Guide

2010 年 8 月 26 日

Text Part Number: OL-21824-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Nexus 5000 トラブルシューティング ガイド

CONTENTS

はじめに

ここでは、『*Cisco Nexus 5000 トラブルシューティング ガイド リリース 1.0*』の対象読者、マニュアルの構成、および表記法について説明します。また、関連資料の入手方法についても説明します。

この章の内容は、次のとおりです。

対象読者

このマニュアルは、Cisco Nexus 5000 シリーズ スイッチの設定や管理を行う熟練ユーザを対象とします。

マニュアルの構成

このリファレンスは、次の章で構成されています。

章	説明
「トラブルシューティングの概要」	Cisco Nexus 5000 シリーズ スイッチの設定および使用時に発生する可能性のある問題のトラブルシューティングについて、基本的な概念、方法、および一般的なガイドラインを紹介します。
「FCoE の問題のトラブルシューティング」	Cisco Nexus 5000 シリーズ スイッチの FCoE で起こり得る問題を特定し、解決する方法について説明します。
「レイヤ 2 スイッチングの問題のトラブルシューティング」	Cisco Nexus 5000 シリーズ スイッチのレイヤ 2 スイッチングで起こり得る問題を特定し、解決する方法について説明します。
「QoS の問題のトラブルシューティング」	Cisco Nexus 5000 シリーズ スイッチの QoS で起こり得る問題を特定し、解決する方法について説明します。

章	説明
「SAN スイッチングの問題のトラブルシューティング」	SAN スイッチングと Cisco Nexus 5000 シリーズ スイッチで起こり得る問題を特定し、解決する方法について説明します。
「セキュリティに関する問題のトラブルシューティング」	Cisco Nexus 5000 シリーズ スイッチのセキュリティで起こり得る問題を特定し、解決する方法について説明します。
「システム管理上の問題のトラブルシューティング」	システム管理と Cisco Nexus 5000 シリーズ スイッチで起こり得る問題を特定し、解決する方法について説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

`screen フォント`	スイッチに表示される端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
`イタリック体の screen フォント`	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ヒント　「*問題解決に役立つ情報*」です。

関連資料

Cisco Nexus 5000 Series スイッチおよび Cisco Nexus 2000 Series Fabric Extender のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

次に、Cisco Nexus 5000 Series および Cisco Nexus 2000 Series Fabric Extender に関連するマニュアルを示します。

『*Cisco Nexus 5000 Series CLI Software Configuration Guide, Cisco NX-OS Release 4.0*』

『*Cisco Nexus 5000 Series NX-OS Command Reference, Cisco NX-OS Release 4.0*』

『*Cisco Nexus 5000 Series Hardware Installation Guide*』

『*Cisco Nexus 5000 Series System Messages Reference*』

『*Cisco Nexus 5000 Series Release Notes*』

『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide, Cisco NX-OS Release 4.1*』

『*Cisco Nexus 2000 Series Fabric Extender Hardware Installation Guide*』

『*Cisco Nexus 5000 Series Fabric Manager Software Configuration Guide, Cisco NX-OS Release 4.0*』

CHAPTER 1

トラブルシューティングの概要

この章では、Cisco Nexus 5000 シリーズ スイッチの設定および使用時に発生する可能性のある問題のトラブルシューティングについて、基本的な概念、方法、および一般的なガイドラインを紹介します。

この章で説明する内容は、次のとおりです。

トラブルシューティングの基本

トラブルシューティングの基本的な手順は次のとおりです。

ステップ 1 特定の現象に関する情報を収集します。

ステップ 2 現象の原因となり得る潜在的な問題をすべて識別します。

ステップ 3 現象が見られなくなるまで、潜在的な問題を系統的に 1 つずつ（最も可能性の高いものから低いものの順に）排除していきます。

起こり得る問題を識別するには、各種ツールを使用するとともに、全体的なコンフィギュレーションを理解する必要があります。このマニュアルの以降の章で、起こり得る問題に対するさまざまなアプローチや具体的な解決方法について説明します。

ベスト プラクティス

ベスト プラクティスとは、スイッチが正常に動作していることを確認するために従う、推奨される手順です。

- すべての Cisco Nexus 5000 スイッチの間で Cisco NX-OS リリースの一貫性を維持します。
- Cisco SAN-OS リリースのリリース ノートを参照して、最新の機能、制限事項、および注意事項を確認します。
- システム メッセージ ロギングをイネーブルにします。
- 変更を実装したら、新しい設定変更のトラブルシューティングを実施します。
- Device Manager を使用して設定を管理し、危険な状況に陥る前に問題を検出します。

共通用語

用語	説明
DCBX	Data Center Bridging Exchange
RSTP+	Rapid Spanning-tree Protocol（高速スパニングツリー プロトコル）
FCoE	FCoE
FCF	Fibre Channel Forwarder（ファイバ チャネル フォワーダ）
FIP	FCoE Initialization Protocol
PFC	PFC
ETS	Enhanced Transmission Selection
LLDP	Link Layer Discovery Protocol
CEE	Converged Enhanced Ethernet
VNTag	Virtual Network Tag（仮想ネットワーク タグ）
ロスレス イーサネット	ドロップのないイーサネット
CNA	Consolidated Network Adaptor（統合ネットワーク アダプタ）
HBA	Host Bus Adaptor（ホスト バス アダプタ）
NPV/NPIV	N-Port Virtualizer（N ポート バーチャライザ））
VN-Link	Virtual Network Link（仮想ネットワーク リンク）
FEX	Fabric Extender（ファブリック イクステンダー）
PAA	Port Analyzer Adaptor（ポート アナライザ アダプタ）
RCF	Reconfigure Fabric
RSCN	Request State Change Notification
Menlo	Cisco FCoE MUX ASIC
FCP	Fibre Channel Protocol（ファイバ チャネル プロトコル）
FSPF	Fabric Shortest Path First

Fabric Manager ツールと CLI コマンド

ここでは、問題のトラブルシューティングによく使用するツールと CLI コマンドについて説明します。これらのツールやコマンドは、状況に応じて特定の問題のトラブルシューティングに使用します。

このマニュアルの以降の章には、その章で取り扱う症状や起こり得る問題に固有のツールやコマンドが追加で示されています。

NX-OS に関するヒント

コンフィギュレーションからの必要な設定情報の表示

```
switch# show running-config interface
version 4.0(1a)N2(1)
```

```
interface vfc29
  no shutdown
  bind interface Ethernet1/29

interface fc2/3
  no shutdown
  switchport speed 1000
  switchport mode SD

interface fc2/4

interface Ethernet1/1
  speed 1000
```

コンフィギュレーション モード内での表示

NX-OS では、コンフィギュレーション モード内から必要なデータを表示できます。そのため、スイッチ プロンプトに戻る必要はありません。

```
switch(config)# show run
switch(config)# show interface brief
```

パイプ コマンド

```
switch# show logging |
  egrep    Egrep
  grep     Grep
  head     Stream Editor
  last     Display last lines
  less     Stream Editor
  no-more  Turn-off pagination for command output
  sed      Stream Editor
  wc       Count words, lines, characters
  begin    Begin with the line that matches
  count    Count number of lines
  exclude  Exclude lines that match
  include  Include lines that match
```

パイプ コマンドを使用して必要なキーワードのみを表示

```
switch# show running-config | include switchport
  system default switchport
  switchport mode trunk
  switchport trunk allowed vlan 1,18
  switchport mode fex-fabric
  switchport mode fex-fabric
  switchport speed 1000
  switchport mode SD
no system default switchport shutdown
```

copy コマンド

```
switch# copy ?
  bootflash:      Select source filesystem
  core:           Select source filesystem
  debug:          Select source filesystem
  ftp:            Select source filesystem
  licenses        Backup license files
  log:            Select source filesystem
  modflash:       Select source filesystem
  nvram:          Select source filesystem
  running-config  Copy running configuration to destination
  scp:            Select source filesystem
  sftp:           Select source filesystem
  startup-config  Copy startup configuration to destination
  system:         Select source filesystem
  tftp:           Select source filesystem
  volatile:       Select source filesystem
```

出力のリダイレクト

NX-OS では、スイッチ上のファイルやフラッシュ エリアに出力をリダイレクトできます。

```
switch# show tech-support aaa > bootflash:ciscolive09

switch# dir
  103557265     Apr 01 17:39:22 2009  .tmp-system
      12451     Apr 10 16:36:37 2009  ciscolive09
      49152     Apr 01 17:39:22 2009  lost+found/
   20058112     Oct 21 13:10:44 2008  n5000-uk9-kickstart.4.0.0.N1.2.bin
   20193280     Apr 01 17:36:37 2009  n5000-uk9-kickstart.4.0.1a.N2.1.bin
   76930262     Oct 21 13:11:33 2008  n5000-uk9.4.0.0.N1.2.bin
  103557265     Apr 01 17:37:30 2009  n5000-uk9.4.0.1a.N2.1.bin
       4096     Jan 01 00:03:26 2005  routing-sw/
```

「tech-support details」コマンドの出力のリダイレクト

「show tech-support details」コマンドの出力をファイルにリダイレクトした後、「tac-pac <filename>」コマンドを使用してそのファイルを gzip で圧縮します。

このファイルは、十分な空きメモリがある場合、bootflash://<filename> に保存されます。ファイル名を指定しなかった場合、作成されるファイルは volatile:show_tech_out.gz になります。前述の「copy コマンド」の項に示す手順に従って、このファイルをデバイスからコピーします。

```
switch# tac-pac
switch# dir volatile:
374382 Aug 16 17:15:55 2010 show_tech_out.gz
```

volatile から、ファイルをブートフラッシュ、FTP、または TFTP サーバにコピーします。

```
switch# copy volatile:show_tech_out.gz ?
bootflash: Select destination filesystem
debug: Select destination filesystem
ftp: Select destination filesystem
log: Select destination filesystem
modflash: Select destination filesystem
```

```
nvram: Select destination filesystem
running-config Copy from source to running configuration
scp: Select destination filesystem
sftp: Select destination filesystem
startup-config Copy from source to startup configuration
system: Select destination filesystem
tftp: Select destination filesystem
volatile: Select destination filesystem
```

NX-OS コマンドの一覧表示

```
switch# show cli list | include ?
  -i    Ignore case difference when comparing strings
  -x    Print only lines where the match is a whole line
  WORD  Search for the expression

switch# show cli list | include debug | include interface
```

キーワードの範囲の絞り込み

grep や include などの各種コマンドを使用して、キーワードの範囲を絞り込むことができます。

```
switch(config-if)# show interface | grep fc
fc2/1 is trunking
fc2/2 is trunking
fc2/3 is up
fc2/4 is down (Administratively down)
vfc29 is up
```

ロギング

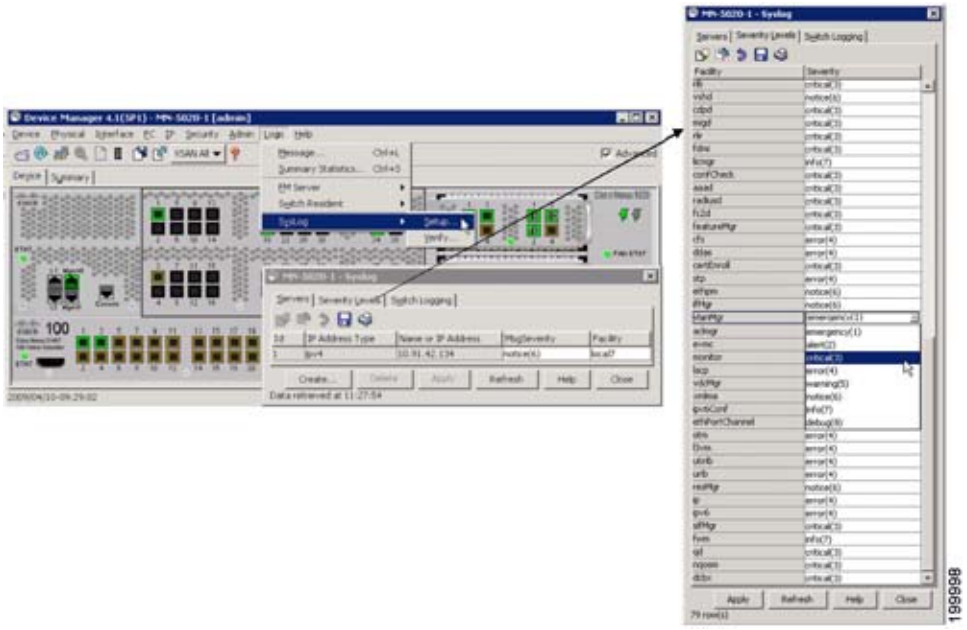
CLI または Device Manager を通じてロギングを使用できます。次に、**logging** コマンドと Device Manager によって重大度情報を表示する例を示します。

CLI での重大度情報の表示

```
switch(config)# show logging

Logging console:                 enabled (Severity: critical)
Logging monitor:                 enabled (Severity: notifications)
Logging linecard:                enabled (Severity: notifications)
Logging fex:                     enabled (Severity: notifications)
Logging timestamp:               Seconds
Logging server:                  enabled
{10.91.42.134}
        server severity:         notifications
        server facility:         local7
        server VRF:              management
Logging logflash:                disabled
Logging logfile:                 enabled
Name - ciscolive09: Severity - debugging Size - 4194304
```

Device Manager での重大度の表示



Ethanalyzer と SPAN

Ethanalyzer は、Nexus 5000 コントロール プレーン宛てのフレーム、または Nexus 5000 コントロール プレーンから発信されたフレームを収集するツールです。このツールによってノードからスイッチへのトラフィック、またはスイッチ間のトラフィックを確認できます。

SPAN は、スイッチにとって一時的なフレームを分析のために別のポートにコピーする機能です。この方法によってノードからスイッチへのトラフィック、またはノード間のトラフィックを確認できます。

Ethanalyzer

Ethanalyzer は、Wireshark オープン ソース コードに基づく Cisco NX-OS プロトコル アナライザ ツールです。このツールは、パケットをキャプチャしてデコードする Wireshark のコマンドライン バージョンです。ネットワークのトラブルシューティングおよびコントロールプレーン トラフィックの分析を実行するために Ethanalyzer を使用できます。

コマンド	説明
ethanalyzer local sniff-interface	スーパーバイザで送信または受信されたパケットをキャプチャし、詳細なプロトコル情報を表示します。
ethanalyzer local sniff-interface brief	スーパーバイザで送信または受信されたパケットをキャプチャし、プロトコル情報の概略を表示します。
ethanalyzer local sniff-interface limit-captured-frames	キャプチャするフレームの数を制限します。
ethanalyzer local sniff-interface limit-frame-size	キャプチャするフレームの長さを制限します。

コマンド	説明
ethanalyzer local sniff-interface capture-filter	キャプチャするパケットのタイプをフィルタリングします。
ethanalyzer local sniff-interface display-filter	表示するキャプチャ済みパケットのタイプをフィルタリングします。
ethanalyzer local sniff-interface decode-internal	Cisco NX-OS の内部フレーム ヘッダーをデコードします。 **（注）** このオプションは、NX-OS Ethanalyzer の代わりに Wireshark を使用してデータを分析する場合には使用しないでください。
ethanalyzer local sniff-interface write	キャプチャしたデータをファイルに保存します。
ethanalyzer local sniff-interface read	キャプチャされたデータ ファイルを開いて分析します。

例

```
switch# ethanalyzer local sniff-interface
No matches in current mode, matching in (exec) mode
  inbound-hi    Inbound(high priority) interface
  inbound-low   Inbound(low priority) interface
  mgmt          Management interface

switch# ethanalyzer local sniff-interface mgmt brief
Capturing on eth0
2008-08-13 01:34:23.776519 10.116.167.244 -> 172.18.217.80 TCP 1106 > telnet [ACK] Seq=0
Ack=0 Win=64040 Len=0
2008-08-13 01:34:23.777752 172.18.217.80 -> 10.116.167.244 TELNET Telnet Data ...
2008-08-13 01:34:23.966262 00:04:dd:2f:75:10 -> 01:80:c2:00:00:00 STP Conf. Root =
32768/00:04:c1:0f:6e:c0  Cost = 57  Port = 0x801d
[省略]
```

次に、Spanning-Tree Protocol（STP; スパニングツリー プロトコル）とファイバ チャネルを表示する例を示します。このコマンドに 0 を指定すると、Ctrl+C を押すまで出力のキャプチャが続きます。FCID はスイッチ ドメイン コントローラの既知の名前です。

```
switch# ethanalyzer local sniff-interface inbound-hi brief limit-captured-frames 0

Capturing on eth4

2008-08-13 01:37:16.639896 00:0d:ec:6b:cd:41 -> 01:80:c2:00:00:00 1 0 00:0d:ec:6b:cd:41 ->
01:80:c2:00:00:00 0x0 0x0 STP RST. Root = 32769/00:0d:ec:6b:cd:41  Cost = 0  Port = 0x8093
2008-08-13 01:37:18.639992 00:0d:ec:6b:cd:41 -> 01:80:c2:00:00:00 1 0 00:0d:ec:6b:cd:41 ->
01:80:c2:00:00:00 0x0 0x0 STP RST. Root = 32769/00:0d:ec:6b:cd:41  Cost = 0  Port = 0x8093

[省略]

2008-08-13 01:37:23.220253 00:0d:ec:6b:cd:40 -> fc:fc:fc:ff:ff:fd 4 0     ff.ff.fd ->
ff.ff.fd     0x5384 0xffff SW_ILS ELP
2008-08-13 01:37:23.220615 00:0d:ec:6b:cd:40 -> aa:bb:cc:dd:01:04 4 0     ff.ff.fd ->
ff.ff.fd     0x5384 0x2b3f FC Link Ctl, ACK1
2008-08-13 01:37:23.227202 00:0d:ec:6b:cd:40 -> aa:bb:cc:dd:01:04 4 0     ff.ff.fd ->
ff.ff.fd     0x5384 0x2b3f SW_ILS SW_ACC (ELP)
2008-08-13 01:37:23.229927 00:0d:ec:6b:cd:40 -> fc:fc:fc:ff:ff:fd 4 0     ff.ff.fd ->
ff.ff.fd     0x5384 0x2b3f FC Link Ctl, ACK1
```

詳細な BPDU

```
switch# ethanalyzer local sniff-interface inbound-hi limit-captured-frames 0
Capturing on eth4
Frame 1 (57 bytes on wire, 57 bytes captured)
    Arrival Time: Aug 13, 2008 01:41:32.631969000
    [Time delta from previous captured frame: 1218591692.631969000 seconds]
    [Time delta from previous displayed frame: 1218591692.631969000 seconds]
    [Time since reference or first frame: 1218591692.631969000 seconds]
    Frame Number: 1
    Frame Length: 57 bytes
    Capture Length: 57 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:vlan:llc:stp]
[省略]
    DSAP: Spanning Tree BPDU (0x42)
    IG Bit: Individual
    SSAP: Spanning Tree BPDU (0x42)
    CR Bit: Command
    Control field: U, func=UI (0x03)
        000. 00.. = Command: Unnumbered Information (0x00)
        .... ..11 = Frame type: Unnumbered frame (0x03)
[省略]
```

SPAN

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによる分析のためにネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe、ファイバ チャネル アナライザ、またはその他の Remote Monitoring（RMON; リモート モニタリング）プローブです。

SPAN 送信元とは、トラフィックをモニタできるインターフェイスを表します。Cisco Nexus 5000 シリーズ スイッチは、SPAN 送信元としてイーサネット、仮想イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VLAN、および VSAN をサポートします。VLAN または VSAN では、指定された VLAN または VSAN でサポートされているすべてのインターフェイスが SPAN 送信元として含まれます。イーサネット、仮想イーサネット、ファイバ チャネル、および仮想ファイバ チャネルの送信元インターフェイスでは、入力方向、出力方向、または両方向の SPAN トラフィックを選択できます。

- 入力送信元（Rx）：この送信元ポートを介してスイッチに入るトラフィックは、SPAN 宛先ポートにコピーされます。
- 出力送信元（Tx）：この送信元ポートを介してスイッチから送信されるトラフィックは、SPAN 宛先ポートにコピーされます。

ソース ポート

送信元ポート（モニタ対象ポートとも呼ばれる）は、ネットワーク トラフィック分析のためにモニタするスイッチド インターフェイスです。スイッチは、任意の数の入力送信元ポート（スイッチで使用できる最大数のポート）と任意の数のソース VLAN または VSAN をサポートします。

ソース ポートは、次の特性を持ちます。

- ポート タイプはイーサネット、仮想イーサネット、ファイバ チャネル、仮想ファイバ チャネル、ポート チャネル、SAN ポート チャネル、VLAN、VSAN のいずれでもかまいません。
- 複数の SPAN セッションではモニタできません。
- 宛先ポートにはなれません。

- 各送信元ポートにモニタする方向（入力、出力、または両方向）を設定できます。VLAN、VSAN、ポート チャネル、および SAN ポート チャネルの送信元の場合、モニタ方向は入力だけであり、グループ内のすべての物理ポートに適用されます。Rx と Tx のオプションは、VLAN または VSAN の SPAN セッションでは使用できません。
- 送信元ポートは、同じ VLAN または VSAN か、別の VLAN または VSAN に設定できます。
- VLAN または VSAN の SPAN 送信元では、ソース VLAN または VSAN のすべてのアクティブ ポートが送信元ポートとして含まれます。
- スイッチは最大 2 つの出力 SPAN 送信元ポートをサポートします。

SPAN 宛先

SPAN 宛先とは、送信元ポートをモニタするインターフェイスを表します。Cisco Nexus 5000 シリーズ スイッチは、SPAN 宛先としてイーサネット インターフェイスとファイバ チャネル インターフェイスをサポートします。

送信元 SPAN	宛先 SPAN
イーサネット	イーサネット
ファイバ チャネル	ファイバ チャネル
ファイバ チャネル	イーサネット（FCoE）
仮想イーサネット	イーサネット
仮想ファイバ チャネル	ファイバ チャネル
仮想ファイバ チャネル	イーサネット（FCoE）

宛先ポートの特性

- 各ローカル SPAN セッション には、送信元ポート、VLAN、または VSAN からトラフィックのコピーを受信する宛先ポート（モニタ ポートとも呼ばれる）がある必要があります。宛先ポートは、次の特性を持ちます。
- 物理ポートはイーサネット、イーサネット（FCoE）、ファイバ チャネルのいずれかを使用できます。仮想イーサネット ポートと仮想ファイバ チャネル ポートは宛先ポートにできません。
- 送信元ポートにはできません。
- ポート チャネルまたは SAN ポート チャネル グループにはできません。
- SPAN セッションがアクティブなときは、スパニング ツリーに参加しません。
- SPAN セッションの送信元 VLAN に属する場合、送信元リストから除外され、モニタされません。
- すべてのモニタ対象送信元ポートの送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ型の場合、輻輳が発生することがあります。この輻輳が、1 つまたは複数のソース ポートでのトラフィック転送に影響を与える場合があります。

モニタに関する注意事項

Nexus 5000 SPAN の特異性

- モニタ（スパン）宛先で COS 値が保持されません。
- モニタ送信元に着信した未知の VLAN タグを持つパケットは、0 の VLAN タグ（プライオリティ タグ）を付けてスパンアウトされます。
- 宛先がイーサネットの場合は、宛先ポートが switchport monitor として設定されている場合にのみ、モニタ セッションがアップします。
- 設定可能な 18 のセッションのうち、アクティブ（アップ ステート）にできるのは 2 つだけです。残りはダウン ステートになります（ハードウェア リソースを使用できません）。

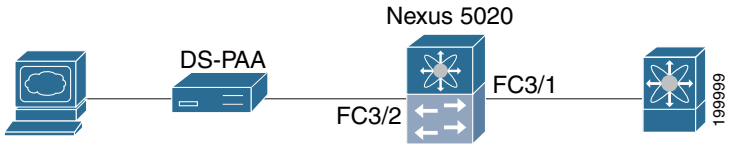
設定に関する制限：VLAN またはポートチャネルを出力送信元として設定できない

- VLAN またはポートチャネルをモニタ宛先にすることはできません。
- 2 つの出力送信元のみがサポートされています。
- あるセッションに対して設定できる宛先ポートは 1 つだけです。

SPAN の設定

例：

```
switch(config)# interface fc3/2
switch(config-if)# switchport mode sd
switch(config-if)# switchport speed 1000
switch(config-if)# no shut
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface fc3/1 tx
switch(config-monitor)# source interface fc3/1 rx
switch(config-monitor)# destination interface fc3/2
```



SPAN セッションの確認

例：

```
switch# show monitor session
SESSION  STATE        REASON                DESCRIPTION
-------  -----------  --------------------  --------------------------------
1        up           The session is up

switch# show monitor session 1
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : fc3/1
    tx            : fc3/1
    both          : fc3/1
```

```
source VLANs      :
    rx            :
source VSANs      :
    rx            :
destination ports : fc3/2
```

SPAN セッションの一時停止

例：

```
switch(config)# monitor session 1 suspend

switch(config)# show monitor session 1
   session 1
---------------
type              : local
state             : down (Session suspended)
source intf       :
    rx            : fc3/1
    tx            : fc3/1
    both          : fc3/1
source VLANs      :
    rx            :
source VSANs      :
    rx            :
destination ports : fc3/2
```

Debugging

コマンドラインでのデバッグ

使用可能なデバッグは、NX-OS でイネーブルにされている機能によって異なります。デバッグをオンにするとき、さまざまなオプションを選択できます。

出力の宛先を決定します。

- ログファイル：スイッチ メモリ内のデータ ファイル。
- コンソール、telnet、または SSH によって画面に直接キャプチャする。

デバッグを実行するには管理者権限が必要です。デバッグは CLI からのみ実行できます。

デバッグ ロギング

debug logfile コマンドを使用し、ログファイルとして CiscoLive_debugs を設定します。設定したデバッグ ファイルの名前を確認するには、**show debug** コマンドを使用します。

```
switch# debug logfile CiscoLive_debugs
switch# show debug
```

デバッグを画面に表示するには、次のコマンドを使用します。

```
switch# show debug logfile CiscoLive_debugs
```

デバッグ ファイルを MDS からサーバにコピーするには、**copy** コマンドを使用します。vrf に入るときに何も指定しなければ、デフォルトが使用されます。

```
switch# copy log:CiscoLive_debugs tftp:

Enter vrf: management
Enter hostname for the tftp server: 10.91.42.134
Trying to connect to tftp server......
Connection to Server Established.
|
TFTP put operation was successful
```

デバッグ ログファイルを削除するには、次のいずれかのコマンドを使用します。

```
switch# clear debug-logfile CiscoLive_debugs

switch# undebug all
```

これらのどのコマンドも使用しない場合は、次のデバッグ ログファイルが作成されるときに既存のデバッグ ログファイルがクリアされ、上書きされます。システムに存在できるデバッグ ログファイルは 1 つだけです。

telnet ウィンドウへの直接のデバッグ

- 予期される出力をバッファまたはファイルにキャプチャする telnet/SSH またはコンソール アプリケーションを使用します。
- トレースをオフにするには、undebug all または特定のデバッグ コマンドの no debug を使用する必要があります。
- 再起動時にはデバッグは保持されません。
- ほとんどのデバッグは解読や理解が容易ですが、中には難解なものもあります。

Cisco Discover Protocol

Cisco Discover Protocol（CDP）バージョン 2 は物理イーサネット インターフェイスに適用され、リンクの両端でイネーブルにした場合にのみ機能します。LLDP 規格は CDP から派生したものです。

CDP は正しいネットワーク デバイスへの適切な接続を確認するために使用され、スイッチ展開では非常に便利です。

次の例は、**show CDP** コマンドで使用できる引数を示します。

```
show cdp
  all           Show interfaces that are CDP enabled
  entry         Show CDP entries in database
  global        Show CDP global parameters
  interface     Show CDP parameters for an interface
  neighbors     Show CDP neighbors
  traffic       Show CDP traffic statistics

switch# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
    Sending DeviceID TLV in Default Format

Device ID:TM-6506-1
System Name:
Interface address(es):
    IPv4 Address: 11.1.1.1
```

```
Platform: cisco WS-C6506, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet1/4, Port ID (outgoing port): TenGigabitEthernet1/2  ? Verifies proper
port connections
Holdtime: 133 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-IPSERVICES_WAN-VM), Version 12.2(18)SXF11, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Fri 14-Sep-07 23:09 by kellythw

Advertisement Version: 2
Native VLAN: 1      ? Sent on Native VLAN
Duplex: full
```

フェールオーバー

FCoE トラフィック

Nexus 5000 でファブリック接続が失われると、影響を受けるすべての vFC インターフェイスがダウンします。

FC ファブリックへの接続の喪失は、次のメカニズムによってホストに通知されます。

- vFC の「シャット」ステートを知らせるため、FIP の「リンク仮想リンクのクリア」が CNA に送られます。「シャット」期間の間、FCF アドバタイズメントによって「ログインできない」ことが通知されます。
- FCoE ネットワーク上で接続が失われた場合は、ログイン セッションをタイムアウトするために、FCF と CNA によって FIP キープアライブが使用されます。キープアライブ タイマーは設定可能です。

非 FCoE トラフィック

ある特定の障害シナリオにおいて、アクセス スイッチが集約レイヤへのアップリンク接続をすべて失った場合は、LAN 接続の喪失を CNA に通知する必要があります。これは、CNA がホスト トラフィックをスタンバイ ポートにフェールオーバーするのに役立ちます。従来、このような障害はホスト向きリンクをダウンさせることによって通知されます。リンクがダウンすると、次の 2 つの目的が達成されます。

- 接続の喪失がホストに通知されます。
- アクセス スイッチが、ホスト向きリンクへのトラフィックの転送、およびホスト向きリンクからのトラフィックの転送を停止します。

ただし、統合ネットワークでは、アクセス スイッチで LAN 接続が失われた場合でも SAN 接続はまだ機能していることがあります。したがって、ホスト向きリンク全体をダウンさせることは望ましくありません。その代わりに、プロトコルによって接続の喪失が通知されます。SAN 接続の喪失は、FIP の「仮想リンクのクリア」メッセージを使用して通知されます。LAN 接続の喪失は、DCBX および VIC プロトコルで定義された論理リンク ステータス TLV を使用して通知されます。

LAN トラフィック

アップリンク上で特定の VLAN の LAN 接続が失われたとき、その VLAN はホスト向きリンク上でもダウンします。

FCoE トラフィック専用の VLAN を作成しておくと、該当するホスト向きリンクへの非 FCoE トラフィック、およびそのホスト向きリンクからの非 FCoE トラフィックをシャットダウンしても、同じホストからの FCoE トラフィックは中断しません。

CHAPTER 2

FCoE の問題のトラブルシューティング

Fibre Channel over Ethernet（FCoE）は、物理イーサネット接続上でファイバ チャネル トラフィックを転送する方式を提供します。FCoE は、全二重とした基本のイーサネットを必要とし、ファイバ チャネル トラフィックのロスレス動作を提供します。

この章では、Cisco Nexus 5000 シリーズ スイッチで FCoe に発生する可能性のある問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。

Data Center Bridging

VFC（FCoE）インターフェイスがオンラインにならない

考えられる原因

FCoE に接続したサーバが、FC または FCoE に接続したストレージに接続できず、このサーバのポートにマップした仮想ファイバ チャネル インターフェイスに対して show interface コマンドを実行すると、その VFC インターフェイスが稼動していないことが報告されます。

解決方法

- 「show running-config」コマンドを使用して設定を確認します。

  例：

（注） VFC のデフォルト設定は停止していますが、次の例ではデフォルト設定をセットアップ スクリプトで変更しています。

```
switch#
feature fcoe
vlan 1
vlan 100
fcoe
```

```
vsan database
vsan 100
interface vfc4
bind interface Ethernet1/4
no shutdown
vsan database
vsan 100 interface vfc4
interface fc2/1
no shutdown
interface Ethernet1/4
switchport mode trunk
switchport trunk allowed vlan 100
spanning-tree port type edge trunk
```

- 該当のインターフェイスで LLDP の送受信がイネーブルになっていることを確認します。
「show lldp interface ethernet 1/4」コマンドを使用します。

  例：

```
switch# show lldp interface ethernet 1/4
Interface Information:
Enable (tx/rx/dcbx): Y/Y/Y Port Mac address: 00:0d:ec:d5:a3:8b
Peer's LLDP TLVs:
Type Length Value
---- ------ -----
001 007 0400c0dd 145486
002 007 0300c0dd 145486
003 002 0078
128 061 001b2102 020a0000 00000002 00000001 04110000 c0000001 00003232
00000000 00000206 060000c0 00080108 100000c0 00890600 1b210889
14001b21 08
000 000
```

  LLDP がディセーブルになっていると VFC はオンラインになりません。
「int ethernet 1/4」コマンドを使用すると、LLDP の送受信をイネーブルにできます。

```
switch(config)# int ethernet 1/4
switch(config-if)# lldp ?
receive Enable LLDP reception on interface
transmit Enable LLDP transmission on interface
```

- 該当のピアで LLDP がサポートされていることを確認します。
リモート ピアが存在するかどうかを確認します。ピアの LLDP TLV の値が存在するかどうかを確認します。
「show lldp interface ethernet 1/4」コマンドを使用します。

  例：

```
switch# show lldp interface ethernet 1/4
Interface Information:
Enable (tx/rx/dcbx): Y/Y/Y Port Mac address: 00:0d:ec:d5:a3:8b
Peer's LLDP TLVs:
Type Length Value
---- ------ -----
001 007 0400c0dd 145486
002 007 0300c0dd 145486
003 002 0078
128 061 001b2102 020a0000 00000002 00000001 04110000 c0000001 00003232
00000000 00000206 060000c0 00080108 100000c0 00890600 1b210889
14001b21 08
```

- ピア（CNA）が DCBX をサポートしているかどうかを確認します。
「show system internal dcbx info interface ethernet 1/4」コマンドを使用します
（4.2(1)N1 よりも前のリリースでは、「sh platform software dcbx internal info interface ethernet x/y」コマンドを使用します）。

（注）　次の例では、DCBX がイネーブルでピアが CEE をサポートしています。

例：

```
switch# show system internal dcbx info interface ethernet 1/4
Interface info for if_index: 0x1a003000(Eth1/4)
tx_enabled: TRUE
rx_enabled: TRUE
dcbx_enabled: TRUE
DCX Protocol: CEE
Port MAC address: 00:0d:ec:d5:a3:8b
DCX Control FSM Variables: seq_no: 0x1, ack_no: 0x2,my_ack_no: 0x1, peer_seq_no: 0x2
oper_version: 0x0, max_version: 0x0 fast_retries 0x0
Lock Status: UNLOCKED
PORT STATE: UP
```

- 「show system internal dcbx info interface ethernet 1/4」コマンドの実行結果で、各ピアの LLDP の値を確認します。
必須の LLDP 値が存在することを確認します。

例：

```
LLDP Neighbors
Remote Peers Information on interface Eth1/4
Remote peer's MSAP: length 12 Bytes:
00 c0 dd 14 54 86 00 c0 dd 14 54 86
LLDP TLV's
LLDP TLV type:Chassis ID LLDP TLV Length: 7
04 00 c0 dd 14 54 86
Chassis type: 04 Chassis ID:00 c0 dd 14 54 86
LLDP TLV type:Port ID LLDP TLV Length: 7
03 00 c0 dd 14 54 86
Port ID subtype: 03 Port ID:00 c0 dd 14 54 86
LLDP TLV type:Time to Live LLDP TLV Length: 2
00 78
TTL = 00
LLDP TLV type:Unknown 128 LLDP TLV Length: 61
00 1b 21 02 02 0a 00 00 00 00 00 02 00 00 00 01 04 11 00 00 c0 00
00 01 00 00 32 32 00 00 00 00 00 00 02 06 06 00 00 c0 00 08 01 08
10 00 00 c0 00 89 06 00 1b 21 08 89 14 00 1b 21 08
LLDP TLV type:END of LLDP PDU LLDP TLV Length: 0
```

- 「show system internal dcbx info interface ethernet 1/4」コマンドの実行結果で、各ピアの DCBX TLV を確認します。
PFC TLV と FCoE TLV の間でネゴシエーションが意図したとおりに実行され、これらがイネーブルになっていること、そこでエラーが発生していないことを確認します。

例：

```
Peer's DCX TLV:
DCBX TLV Proto(1) type: 1(Control) DCBX TLV Length: 10 DCBX TLV Value
00 00 02 00 00 00 01 00 00 00
sub_type 0, error 0, willing 0, enable 0, max_version 0, oper_version 0
DCBX TLV Proto(1) type: 2(PriGrp) DCBX TLV Length: 17 DCBX TLV Value
00 00 c0 00 00 01 00 00 32 32 00 00 00 00 00 00 02
sub_type 0, error 0, willing 1, enable 1, max_version 0, oper_version 0
```

```
DCBX TLV Proto(1) type: 3(PFC) DCBX TLV Length: 6 DCBX TLV Value
00 00 c0 00 08 01
sub_type 0, error 0, willing 1, enable 1, max_version 0, oper_version 0
DCBX TLV Proto(1) type: 4(App(Fcoe)) DCBX TLV Length: 16 DCBX TLV Value
00 00 c0 00 89 06 00 1b 21 08 89 14 00 1b 21 08
sub_type 0, error 0, willing 1, enable 1, max_version 0, oper_version 0
```

- ピアの PFC と FCoE のサブタイプを確認します。

  「show system internal dcbx info interface ethernet 1/4」コマンドを使用します (4.2(1)N1 よりも前のリリースでは、「sh platform software dcbx internal info interface ethernet x/y」コマンドを使用します)。

  例：

```
Feature type PFC (3)
feature type 3(PFC)sub_type 0
Feature State Variables: oper_version 0 error 0 local error 0 oper_mode 1
feature_seq_no 0 remote_feature_tlv_present 1 remote_tlv_aged_out 0
remote_tlv_not_present_notification_sent 0
Feature Register Params: max_version 0, enable 1, willing 0 advertise 1
disruptive_error 0 mts_addr_node 0x101 mts_addr_sap 0x179
Desired config cfg length: 2 data bytes:08 08
Operating config cfg length: 2 data bytes:08 08
Peer config cfg length: 0 data bytes:
Feature type App(Fcoe) (4)sub_type FCoE (0)
feature type 4(App(Fcoe))sub_type 0
Feature State Variables: oper_version 0 error 0 local error 0 oper_mode 1
feature_seq_no 0 remote_feature_tlv_present 1 remote_tlv_aged_out 0
remote_tlv_not_present_notification_sent 0
Feature Register Params: max_version 0, enable 1, willing 0 advertise 1
disruptive_error 0 mts_addr_node 0x101 mts_addr_sap 0x179
```

- 「show system internal dcbx info interface ethernet 1/4」コマンドを実行して表示された結果の末尾にある DCBX カウンタを確認します。何らかのエラーが記録されていないか調べます。

  例：

```
Traffic Counters
DCBX pkt stats:
Total frames out: 15383
Total Entries aged: 97
Total frames in: 15039
DCBX frames in: 15033
Total frames received in error: 6
Total frames discarded: 6
Total TLVs unrecognized: 0
```

- FCoE の Data Center Bridging についても同様の値を確認し、ホストの CNA ソフトウェアで Type-Length-Value を確認します。

解決方法のまとめ

- 各機能のネゴシエーション結果を確認します。

  「show system internal dcbx info interface ethernet 1/4」コマンドを使用します (4.2(1)N1 よりも前のリリースでは、「sh platform software dcbx internal info interface ethernet x/y」コマンドを使用します)。

  例：

```
feature type 3 sub_type 0
feature state variables: oper_version 0 error 0 oper_mode 1 feature_seq_no 0
remote_feature_tlv_present 1
remote_tlv_not_present_notification_sent 0 remote_tlv_aged_out 0
```

```
feature register params max_version 0, enable 1, willing 0 advertise 1,
disruptive_error 0 mts_addr_node
0x101mts_addr_sap 0x1e5
Desired config cfg length: 1 data bytes:08
Operating config cfg length: 1 data bytes:08
```

- エラー
  - ネゴシエーションのエラーが発生しています。
  - CNA に接続するときに発生するとは考えられません。
  - 2 台の Nexus 5000 スイッチをバックツーバックで接続している場合は、複数の異なる CoS 値に対して PFC をイネーブルにすると、ネゴシエーションのエラーが発生することがあります。
- 動作設定
  - ネゴシエーションの結果を示します。
  - 動作設定が存在しない場合は、ピアが DCBX TLV をサポートしていないか、ネゴシエーションのエラーが発生しています。
  - 「remote_feature_tlv_present」は、リモート ピアがこの機能の TLV をサポートしているかどうかを示しています。
- 次の理由で、DCBX 機能が稼動していない可能性があります。
  - ピアが LLDP プロトコルをサポートしていない。
  - ピアが DCBX プロトコルをサポートしていない。
  - ピアが一部の DCBX TLV をサポートしていない。
  - DCBX のネゴシエーションで予期しない結果が得られた。
- インターフェイスに PFC モードを強制的に適用するオプションが用意されています。PFC モードを強制的に適用するには、「switch(config)# int eth1/21」コマンドと「switch(config-if)# priority-flow-control mode ?」コマンドを使用します。

  例：

```
switch(config)# int eth1/21
switch(config-if)# priority-flow-control mode ?
auto Advertise priority-flow-control capability
on Turn on priority-flow-control
```

（注） 上記のコマンドのデフォルト設定は「auto」です。「no」オプションを指定すると、モードは「auto」に戻ります。

FIP

（注） Nexus 2232 FEX では、FIP Generation-1 CNA がサポートされていません。Nexus 2232 FEX では、FIP Generation-2　CNA のみがサポートされています。

FIP の障害が原因で VFC が停止する

FIP に関連する TLV をホストがサポートしていません。

考えられる原因

接続先のホストが FIP をサポートしていない場合は、起動する VFC に応じて VLAN 検出の最初の手順が失敗します。FIP で必要となる 3 種類の基本的な TLV が、バインドしたインターフェイス経由で DCBX によって交換されていること、および FIP で FCOE-MGR がイネーブルになっていることを、以下のコマンドを使用して確認します。この 3 種類の TLV とは、FCoE TLV、PriGrp TLV、および PFC TLV です。ローカルとピアの両方について、これら 3 種類の TLV の値が存在していることを確認する必要があります。

次のコマンドを使用して TLV を確認します。

- 「show system internal dcbx info interface <bound-ethernet-interface-id>」
- 「show platform software fcoe_mgr info interface vfc<id>」

これらのコマンドの実行結果に「FIP Capable ?: TRUE」および「Triggered event: [FCOE_MGR_VFC_EV_FIP_VLAN_DISCOVERY]」が表示されているかどうかを確認します。

VFC は、これ以上進行しない状態となり、要求を受け取ることができません。

解決方法

FIP をサポートしている適切なファームウェアとドライバを CNA で使用していること、および FIP をサポートしているアダプタを使用していることを確認します。

FIP 要求の障害が原因で VFC が停止する

FIP 要求が失敗すると、VFC が停止します。

考えられる原因

FIP VLAN 検出の最初の手順が成功すると、ホストは FIP 要求を送信します。スイッチでは、この要求に対して詳細な FIP アドバタイズメントを使用して応答する必要があります。この応答を送信しなかった場合、または受信した要求に対してアドバタイズメントを返信しなかった場合、VFC は動作を開始しません。ホストは要求を継続しようとしますが、成功することはありません。

応答やアドバタイズメントが得られない理由として、以下が考えられます。

- アクティブなファブリックが提供する MAC アドレスが存在しない（FC マップが正しくない場合など）。
- FLOGI で使用できるファブリックが存在しない。
- MAC アドレス記述子が正しくない（これは、CNA が応答を送信するときに DMAC として使用するアドレスです）。

「show platform software fcoe_mgr info interface vfc<id>」コマンドを使用して、FIP 要求のステータスを表示します。

このコマンドの実行結果で、「Triggered event: [FCOE_MGR_VFC_EV_FIP_VLAN_DISCOVERY]」に続いて

「Triggered event: [FCOE_MGR_VFC_EV_FIP_SOLICITATION]」が表示されている部分を確認します。

要求が成功している場合は、これに続いて「Triggered event: [FCOE_MGR_VFC_EV_FIP_FLOGI]」が表示されています。

要求が失敗している場合は「Triggered event: [FCOE_MGR_VFC_EV_FIP_FLOGI]」が表示されず、これ以上の処理は行われません。

解決方法

VSAN がアクティブであること、メンバーシップが正しいこと、およびファブリックが使用可能であることを確認する必要があります。また、NPV モードで、アクティブな境界ポートや NP ポートが存在することを確認します。

VLAN からの応答を CNA で受信できないために VFC が停止する

スイッチからは VLAN 応答が送信されていますが、それが CNA で受信されません。これは VFC が動作していないためです。

考えられる原因

バインドしたインターフェイスのネイティブ VLAN ID は、FCoE VLAN のものではないことが必要です。この ID が FCoE VLAN のもので、ネイティブ VLAN がその FCoE VLAN に一致していると、送信される VLAN 応答はタグなしになります。一方、FIP アダプタではタグ付きのフレームを受信することを想定しています。したがって、トランク インターフェイス上のネイティブ VLAN は FCoE VLAN ではないことが必要になります。

解決方法

バインドしたイーサネット トランク インターフェイスの設定を調べ、ネイティブ VLAN が FCoE VLAN ではないでことを確認します。

バインドしたイーサネット インターフェイス上にアクティブな STP ポート ステートが存在しないために、VFC が停止する

バインドしたイーサネット インターフェイス上にアクティブな STP ポート ステートが存在しないために、VFC が停止します。

考えられる原因

ネイティブ VLAN と、アクティブな VSAN にマップしたメンバ FCoE VLAN の両方で、バインドしたインターフェイスは STP フォワーディング ステートにあることが必要です。STP のアクティブなポートが VLAN 上に存在しないと、バインドしたインターフェイスを介してその VLAN で受信した FIP パケットはすべてスイッチでドロップされます。その結果、FIP による VFC の起動が始まりません。

解決方法

FCoE ではないネイティブ VLAN と FCoE であるメンバ VLAN の両方で、バインドしたイーサネット トランク インターフェイス上の STP ポート ステートを確認します。STP ポート ステートが、ブロックした不整合なステートまたはエラー ディセーブル ステートにある場合は、それを修復してフォワーディング ステートに移行します。

FIP のキープアライブが欠落するために VFC が停止する

FIP のキープアライブが欠落するために VFC が停止します。

考えられる原因

FIP のキープアライブ（FKA）が 22 秒ほど欠落すると、ほぼ 3 回連続でホストから FKA が受信されていないことになります。FKA の欠落が発生する原因は、輻輳やリンク上の問題などさまざまです。

FKA のタイムアウトは、FKA の平均周期（FKA_adv_period）を 2.4 倍した値です。

FKA_adv_period は、要求に応答する FIP アドバタイズメントの際にホストの間で取り交わされ、合意されます。

次のコマンドの実行結果を検討して、FKA の欠落が発生しているかどうかを確認します。

- 「show platform software fcoe_mgr info interface vfc<id>」
- 「show platform software fcoe_mgr event-history errors」
- 「show platform software fcoe_mgr event-history lock」
- 「show platform software fcoe_mgr event-history msgs」
- 「show platform fwm info pif ethernet <bound-ethernet-interface-id>」

解決方法

輻輳が解消されると、VFC は復旧します。症状が継続する場合は、さらに分析が必要になります。その場合に考慮すべき点は次のとおりです。

- ホストが FKA の送信を停止している。
- 受信した FKA をスイッチがドロップしている。

CNA

ここでは、Converged Network Adapter（CNA; 統合ネットワーク アダプタ）のトポロジのベスト プラクティス概要、ホストで使用するツールによるトラブルシューティングの説明、および一般的な問題の説明とその解決方法を取り上げます。

CNA のベスト プラクティス トポロジ

直接接続した CNA のベスト プラクティス トポロジ

- SAN の各仮想ファブリック（VSAN）にトラフィックを伝送するように、すべての統合アクセス スイッチでそれぞれに専用の VLAN を設定する必要があります（VSAN 1 では VLAN 1002、VSAN 2 では VLAN 1003 など）。MSTP がイネーブルである場合、FCoE VLAN では独立した MST インスタンスを使用する必要があります。
- Unified Fabric（UF; 統合ファブリック）のリンクはトランク ポートとして設定する必要があります。FCoE VLAN は、ネイティブ VLAN として設定しないようにします。すべての FCoE VLAN は、UF リンクのメンバーとして設定する必要があります。これにより、VFC インターフェイスでの VF_Port トランキングと VSAN 管理のために FCoE VLAN を拡張できるようになります。
- UF リンクは、スパニングツリー エッジ ポートとして設定する必要があります。
- FCoE VLAN は、FCoE トラフィックの伝送用として指定していないイーサネット リンクのメンバーとして設定しないようにします。これにより、FCoE VLAN で使用するスパニングツリー プロトコルの範囲を UF リンクのみに制限できます。
- 統合アクセス スイッチを（それが存在する SAN ファブリックに関係なく）、LAN の代替パスを設定する目的でイーサネット経由の各リンクに接続する必要がある場合は、すべての FCoE VLAN をメンバーシップから除外するようにこれらのリンクを明示的に設定する必要があります。これにより、FCoE VLAN で使用するスパニングツリー プロトコルの範囲を UF リンクのみに制限できます。
- SAN-A および SAN-B の FCoE には別の FCoE VLAN を使用する必要があります。

リモート接続した CNA のベスト プラクティス トポロジ

- SAN の各仮想ファブリック（VSAN）にトラフィックを伝送するように、すべての統合アクセス スイッチおよびすべてのブレード スイッチでそれぞれに専用の VLAN を設定する必要があります（VSAN 1 では VLAN 1002、VSAN 2 では VLAN 1002 など）。MSTP がイネーブルである場合、FCoE VLAN では独立した MST インスタンスを使用する必要があります。
- Unified Fabric（UF; 統合ファブリック）のリンクはトランク ポートとして設定する必要があります。FCoE VLAN は、ネイティブ VLAN として設定しないようにします。すべての FCoE VLAN は、UF リンクのメンバとして設定する必要があります。これにより、VFC での VF_Port トランキングと VSAN 管理のために FCoE VLAN を拡張できるようになります。
- CNA とブレード スイッチ間の UF リンクは、スパニングツリー エッジ ポートとして設定する必要があります。
- 各ブレード スイッチを接続する統合アクセス スイッチは 1 台のみとする必要があります。新しいリンクやブレード スイッチのプロビジョニングなどで実行する STP の再コンバージェンスによって中断が発生しないように、可能な限り、この接続はイーサネット ポート チャネル経由とします。

ホスト ツールによるトラブルシューティング

以下は、ホストで使用するツールで CNA のトラブルシューティングを実行する際の注意事項です。

- Emulex
  - Emulex には、Emulex の CNA を管理する「OneCommand」GUI ツールが用意されています。このツールの [CEE] タブには、DCB 設定の詳細および FC インターフェイスの FIP 設定の詳細が表示されます。
- Qlogic
  - Qlogic には「SanSurfer」ツールが用意されています。このツールの [Data Center Bridging] タブには、スイッチから学習した、TLV 交換データのみの DCB 設定が表示されます。このツールの [DCE Statistics] タブには、イーサネットの統計情報が表示されます。
- Microsoft Windows
  - Microsoft Windows には、数多くの CNA ベンダー製品の設定とレジスタを表示するツールが用意されています。

ホスト OS で CNA を認識できない

Converged Network Adapter（CNA; 統合ネットワーク アダプタ）はホストにインストールされていますが、その CNA を認識できません。

考えられる原因

インストールした CNA のモデルをサポートする適切なドライバがホストのオペレーティング システムに存在していない可能性があります。

解決方法

ステップ 1　1）次の情報を収集します。

a. ホストのオペレーティング システム。

b. インストールした CNA の具体的なモデル名。

ステップ 2　CNA モデルとホスト OS について、各ベンダーの適切なサポート ページを調べます。

ステップ 3　既存のドライバがホスト OS にインストールされているかどうかを確認します。

ステップ 4　CNA ベンダーのサポート ページまたはホスト OS のサポート ページから最新のドライバをインストールしていることを確認します。

PFC

ここでは、標準ポーズ フレームの表示方法を簡単に紹介し、一般的な問題とその解決方法について説明します。

標準ポーズ フレーム

Nexus 5000 では、CNA ではない標準のホスト接続を備えたポートに対して標準ポーズ フレームをサポートしています。この標準ポーズ フレームは、次の例にあるようにインターフェイスの設定でイネーブルにできます。

例：

```
switch(config)# int eth 1/16
switch(config-if)# flowcontrol ?
     receive  Receive pause frames
     send     Send pause frames
switch(config-if)# flowcontrol receive on
switch(config-if)# flowcontrol send on
```

標準ポーズ フレームを表示するには、「show interface flowcontrol」コマンドを使用します。

例：

```
switch(config-if)# sh int flowcontrol

--------------------------------------------------------------------------------
Port      Send      FlowControl    Receive   FlowControl    RxPause   TxPause
          admin         oper       admin       oper
--------------------------------------------------------------------------------
Eth1/1    off           off        off         off          0         0
Eth1/2    off           off        off         off          0         0
Eth1/3    off           off        off         off          0         0
Eth1/4    off           off        off         off          0         0
Eth1/5    off           off        off         off          0         0
Eth1/6    off           off        off         off          0         0
Eth1/7    off           off        off         off          0         0
Eth1/8    off           off        off         off          0         0
Eth1/9    off           off        off         off          0         0
Eth1/10   off           off        off         off          0         0
Eth1/11   off           off        off         off          0         0
Eth1/12   off           off        off         off          0         0
Eth1/13   off           off        off         off          0         0
Eth1/14   off           off        off         off          0         0
Eth1/15   off           off        off         off          0         0
Eth1/16   on            on         on          on           0         0
Eth1/17   off           off        off         off          0         0
```

PFC が FCoE 対応アダプタ（CNA）とネゴシエートしない

Priority Flow Control（PFC; プライオリティ フロー制御）が、FCoE 対応アダプタ（CNA）とネゴシエートしません。

その結果、サーバからの FCoE トラフィックにパケットのドロップが発生します。

考えられる原因

CNA が DCBX をサポートしていないために、PFC TLV がネゴシエートされていない可能性があります。

解決方法

次の手順を実行して、DCBX のサポート状況を調べ、PFC TLV がネゴシエートされていることを確認します。

- PFC のステータスを確認します。「show int ethx/x priority-flow-control」コマンドを使用します（CNA に接続します）。

  例：

```
switch# show int eth1/13 priority-flow-control
===============================================================
Port               Mode Oper(VL bmap)  RxPPP      TxPPP
===============================================================

Ethernet1/13       Auto Off         0          0
```

- ピアでアドバタイズされた LLDP ネイバーまたは PFC/DCBX TLV が存在するかどうかを確認します。「show system internal dcbx info int ethx/x」コマンドを使用します。

  例：

```
switch(config-if)# show system internal dcbx info interface eth1/1

Interface info for if_index: 0x1a000000(Eth1/1)
tx_enabled: FALSE
rx_enabled: FALSE
dcbx_enabled: TRUE
DCX Protocol: CIN


Port MAC address:  00:0d:ec:c9:c8:08


DCX Control FSM Variables: seq_no: 0x1, ack_no: 0x0,my_ack_no: 0x0, peer_seq_no:
 0x0 oper_version: 0x0,  max_version: 0x0 fast_retries 0x0

Lock Status: UNLOCKED
PORT STATE: UP
LLDP Neighbors
No DCX tlvs from the remote peer
```

- ピアが DCBX をサポートしていない場合は、プライオリティ フロー制御のモード設定を「on」にして PFC をイネーブルにします。

CNA に接続したスイッチ インターフェイスで継続的なポーズ フレーム（PFC）が受信される

CNA にスイッチ インターフェイスを接続すると、継続的なポーズ フレーム（PFC）が受信されます。

考えられる原因

Nexus 5000 スイッチを CNA に接続している場合は、その CNA からスイッチに Xon PFC フレームが送信されていることがあります。これにより、「show interface ethx/x」コマンドを発行するとポーズ カウンタの値が増加します。

この状況を確認するには、次の手順を実行します。

- 「show interface ethx/x」コマンドを数回実行し、「show interface ethx/x |grep - i pause」コマンドを使用して、ポーズ フレームのカウントが増加していることを確認します。
- 「show interface ethx/x」コマンドを数回実行し、「show interface ethx/x priority-flow-control」コマンドを使用して、PFC フレームのカウントが増加していることを確認します。
- 「show queuing interface ethx/x」コマンドを数回発行して、ポーズのステータスを確認します。

  例：

  ```
  Per-priority-pause status                 : Rx (Inactive), Tx (Inactive)
  ```

  「show interface ethx/x priority-flow-control」コマンドの実行結果で Rx（Inactive）とポーズ カウンタが時間とともに増加している場合、この問題の原因は CNA から送信される Xon フレームです。

考えられる原因

スイッチ ポートからのトラフィックを処理できない低速なサーバが Nexus 5000 と SNA との接続に関係している場合、そのサーバは、スイッチの動作速度を下げるために Xoff ポーズ フレームをスイッチに送信します。これにより、「show interface ethx/x」コマンドを使用するとポーズ カウンタの値が増加します。

この状況を確認するには、次の手順を実行します。

- 「show interface ethx/x |grep - i pause」コマンドを数回実行して、ポーズ フレームのカウントが増加していることを確認します。
- 「show interface ethx/x priority-flow-control」コマンドを数回実行して、PFC フレームのカウントが増加していることを確認します。
- 「show queuing interface ethx/x」コマンドを数回発行して、ポーズのステータスを確認します。

  例：

  ```
  Per-priority-pause status                 : Rx (Active), Tx (Inactive)
  ```

「show interface ethx/x priority-flow-control」コマンドの実行結果で Rx（Active）とポーズ カウンタが増加している場合、この問題の原因はサーバから送信される Xoff フレームです。

解決方法

サーバから Xoff ポーズ フレームが送信されると、Nexus 5000 のインターフェイスが一時停止し、スイッチから CNA へのスループットが低下します。サーバの OS と PCI スロットを調べ、高速なサーバとして機能しているかどうかを確認します。サーバを、10G のスループットを実行できるものに入れ替えます。

スイッチがポーズ フレームを送信しているかどうか、または一時停止しているかどうかの確認

スイッチからポーズ フレームが送信されているために、サーバで FCoE のスループットがきわめて低くなっています。スイッチがポーズ フレームを送信しているかどうか、または一時停止しているかどうかの確認が必要です。

考えられる原因

出力 FC ポートで輻輳が発生していると、スイッチからサーバに PFC フレームが送信されます。FCoE のレートを下げ、パケットのドロップを避けるために PFC フレームが送信されます。サーバの処理速度が低下した場合やサーバに輻輳が発生した場合、サーバからスイッチ インターフェイスに PFC フレームが送信されます。

この状況を確認するには、次の手順を実行します。

- 「show interface ethx/x |grep - i pause」コマンドを数回実行して、ポーズ フレームのカウント（Rx/TX）が増加していることを確認します。
- 「show interface ethx/x priority-flow-control」コマンドを数回実行して、PFC フレームのカウント（RX/TX）が増加していることを確認します。
- 「show queuing interface ethx/x」コマンドを数回使用して、ポーズのステータスを確認します。

（注）　PFC フレームは MAC レベル タイプのパケットなので、SPAN 機能では表示できません。回線で伝送されている実際の PFC フレームを確認するには、インラインのアナライザが必要です。

例：

```
Per-priority-pause status                 : Rx (Active), Tx (Inactive)
```

「show interface ethx/x priority-flow-control」コマンドの実行結果で RX（Active）とポーズ RX カウンタが増加している場合、この問題の原因はサーバから送信される Xoff フレームです。

「show interface ethx/x priority-flow-control」コマンドの実行結果で Tx（Active）とポーズ TX カウンタが増加している場合、この問題の原因はスイッチによって転送される Xoff フレームです。

解決方法

輻輳の発生源を突き止め、FC の帯域幅を引き上げるか、サーバを高性能なものに入れ替えることで、輻輳を解決します。輻輳の発生が予想される場合は、FCoE トラフィックにポーズが発生すると考えるべきです。

ポーズ レートの限度によってスイッチ ポートが err-disabled になる

ポーズ レートに限度があることから、スイッチ ポートが err-disable ステートになります。

考えられる原因

スイッチ インターフェイスがサーバから過剰な Xoff ポーズ フレームを受信すると、ポーズ フレームのレートが高すぎるためにそのスイッチのポートが error-disabled ステートになります。通常は、10G ポートでの送信速度が 5mbps を下回っている場合にのみ、ポーズ フレームによってポートが err-disable ステートになります。これは、サーバの処理速度が大幅に低下し、大量のポーズ フレームがスイッチのポートに送信されている状態です。

この状況を確認するには「show int eth1/14 brief」コマンドを使用します。

例：

```
--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/14   110    eth  trunk  down    pauseRateLimitErrDisable    100(D) 110
```

- RX ポーズ カウントが大きな値になっていることを確認します。「show interface ethx/x」コマンドを使用してポーズ カウンタを表示します。
- 「show hardware internal gatos event-history errors |grep -i err」コマンドを使用して、ポーズの err-disable ログを確認します。

解決方法

次のような一時的な条件によってポートが err-disabled になっている場合は、ポーズの err-disable 回復をイネーブルにして、ポートをこのステートから解放できます。

次の一時的な条件によってポートが err-disabled になっている場合は、ポーズの err-disable 回復をイネーブルにして、ポートをこのステートから解放できます。

- err-disable 回復によってポーズ レート限度が発生している。
- err-disable 回復の間隔が 30 である。

ポーズ レートの限度によってポートが一貫して err-disabled ステートになっている場合は、低速なサーバが問題であるかどうかを判断します。低速なサーバを高速なサーバに入れ替えます。

DCBX 対応デバイスに接続したスイッチでリンク ポーズ（フロー制御）をイネーブルにする方法

サーバに接続したスイッチのポートでリンク ポーズがイネーブルになりません。DCBX 対応デバイスに接続した Nexus 5000 スイッチではリンク ポーズ（フロー制御）がイネーブルであることが必要です。

考えられる原因

ピアが DCBX で PFC TLV をサポートしている場合は、「flowcontrol send on」および「flowcontrol receive on」を設定するとリンク ポーズがイネーブルになりません。該当のインターフェイス上で DCBX が送信する PFC TLV をディセーブルにする必要があります。

この状況を確認するには、次のいずれかの手順を実行します。

- 「show interface ethx/y flowcontrol」コマンドを使用して、動作ステートがオフであるかどうかを確認します。
- 「show interface ethx/y priority-flow-control」コマンドを使用して、動作ステートがオンであるかどうかを確認します。

解決方法

「interface ethx/y」で次のコマンドを使用して、DCBX 対応デバイスで PFC の代わりにリンク ポーズをイネーブルにします。

- 「no priority-flow-control mode on」
- 「flowcontrol receive on」
- 「flowcontrol send on」

PFC カウンタをクリアする方法

プライオリティ フロー カウンタをクリアする方法。

考えられる原因

現在のところ、PFC フレームをクリアする CLI コマンドはありません（バグ ID CSCtg08068）。

解決方法

PFC カウンタをクリアする CLI コマンドはありませんが、クリアする方法はあります。インターフェイス カウンタをクリアしてから「show interface ethx/x flowcontrol」コマンドを発行すると、PFC フレームのカウントを表示できます。

（注）「show int ethx/x flowcontrol」コマンドを使用すると PFC フレームのカウントが増加します。これは既知のバグです。

レジスタとカウンタ

インターフェイス レベルのエラー

インターフェイス レベルのエラーを表示するには「show interface counters errors」コマンドを使用します。

例：

```
switch# show interface counters errors

--------------------------------------------------------------------------------
Port      Align-Err      FCS-Err   Xmit-Err  Rev-Err   Undersize     OutDiscards
--------------------------------------------------------------------------------
Eth1/1            0            0          0        0            0               0
Eth1/2            0            0          0        0            0               0
Eth1/3            0            0          0        0            0               0
Eth1/4            0            0          0        0            0               0
Eth1/5            0            0          0        0            0               0
Eth1/6            0            0          0        0            0               0
Eth1/7            0            0          0        0            0               0
Eth1/8            0            0          0        0            0               0
Eth1/9            0            0          0        0            0               0
Eth1/10           0            0          0        0            0               0
Eth1/11           0            0          0        0            0               0
Eth1/12           0            0          0        0            0               0
Eth1/13           0            0          0        0            0               0
Eth1/14           0            0          0        0            0               0
Eth1/15           0            0          0        0            0               0
Eth1/16           0            0          0        0            0               0
Eth1/17           0            0          0        0            0               0
Eth1/18           0            0          0        0            0               0
Eth1/19           0            0          0        0            0               0
Eth1/20           0            0          0        0            0               0
Eth2/1            0            0          0        0            0               0
Eth2/2            0            0          0        0            0               0
Eth2/3            0            0          0        0            0               0
Eth2/4            0            0          0        0            0               0
Po300             0            0          0        0            0               0
mgmt0            --           --         --       --           --              --
```

パケットのバイト数

パケットのバイト数を表示するには「show interface counters detailed」コマンドを使用します。

例：

```
sh interface ethernet  1/11 counters detailed

Ethernet 1/11
  Rx Packets:                                     430908
  Rx Unicast Packets:                             129965
  Rx Multicast Packets:                           300932
  Rx Broadcast Packets:                               11
  Rx Jumbo Packets:                                    3
  Rx Bytes:                                     41893521
  Rx Packets from 0 to 64 bytes:                      47
  Rx Packets from 65 to 127 bytes:                353478
  Rx Packets from 128 to 255 bytes:                60265
  Rx Packets from 256 to 511 bytes:                17095
  Rx Packets from 512 to 1023 bytes:                  16
  Rx Packets from 1024 to 1518 bytes:                  4
  Rx Trunk Packets:                               387901
  Tx Packets:                                     172983
  Tx Unicast Packets:                             129959
  Tx Multicast Packets:                            43024
  Tx Jumbo Packets:                                    3
  Tx Bytes:                                     18220330
  Tx Packets from 0 to 64 bytes:                       7
  Tx Packets from 65 to 127 bytes:                112452
  Tx Packets from 128 to 255 bytes:                60461
  Tx Packets from 256 to 511 bytes:                   40
  Tx Packets from 512 to 1023 bytes:                  19
  Tx Packets from 1024 to 1518 bytes:                  1
  Tx Trunk Packets:                               130019
```

SNMP 読み取りの検証

SNMP 読み取りの検証を表示するには「sh interface ethernet 1/11 counters snmp」コマンドを使用します。

例：

```
switch# sh interface ethernet 1/11 counters snmp

--------------------------------------------------------------------------------
Port               InOctets                    InUcastPkts
--------------------------------------------------------------------------------
Eth1/11            41908130                      130009

--------------------------------------------------------------------------------
Port               InMcastPkts                 InBcastPkts
--------------------------------------------------------------------------------
Eth1/11              301038                           11

--------------------------------------------------------------------------------
Port               OutOctets                   OutUcastPkts
--------------------------------------------------------------------------------
```

```
Eth1/11            18226503                          130003

--------------------------------------------------------------------------------
Port               OutMcastPkts                  OutBcastPkts
--------------------------------------------------------------------------------
Eth1/11               43039                             0
```

トラフィック レート

トラフィック レートを表示するには「sh interface ethernet 1/11 counters brief」コマンドを使用します。

例：

```
switch# sh interface ethernet 1/11 counters brief

-------------------------------------------------------------------------------
Interface          Input Rate (avg)    Output Rate (avg)
                   ----------------    -----------------
                   Rate      Total     Rate      Total          Rate averaging
                   MB/s      Frames    MB/s      Frames         interval (seconds)
-------------------------------------------------------------------------------
Ethernet 1/11      0         0         0         0              30
                   0         0         0         0              300
```

CHAPTER 3

レイヤ 2 スイッチングの問題のトラブルシューティング

レイヤ 2 は、コンピュータ ネットワーキングの Open Systems Interconnection（OSI）モデルのデータ リンク層です。

この章では、Cisco Nexus 5000 シリーズ スイッチのレイヤ 2 スイッチングで起こり得る問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。

MAC アドレス テーブル

データ トラフィックのフラッディング

データが転送されず、代わりに VLAN のすべてのポートにフラッディングされます。

考えられる原因

ループの検出が原因で、MAC アドレスの学習がディセーブルになっています。この場合は、重大度 2 の Syslog メッセージ、STM_LOOP_DETECT が受信されています。

解決方法

180 秒待機した後、学習が自動的にイネーブルになります。重大度 2 の Syslog メッセージ、STM_LEARNING_RE_ENABLE が受信されます。

考えられる原因

MAC アドレス テーブルがいっぱいになっています。この場合は、重大度 2 の Syslog メッセージ、STM_LIMIT_REACHED が受信されています。

解決方法

180 秒待機した後、MAC テーブルがフラッシュされ、学習が自動的にイネーブルになります。あるいは、一部の MAC エントリの期限が切れて学習済みエントリの総数が 1500 より少なくなるまで待つか、「clear mac address-table dynamic [address <mac>]」コマンドを実行してエントリをクリアします。こうすると、新しい MAC エントリを学習するための空き領域が作成されます。重大度 2 の Syslog メッセージ、STM_LEARNING_RE_ENABLE が受信されます。

考えられる原因

学習の過負荷が原因で（つまり、新しいアドレスが短時間であまりにも多すぎたため）、MAC アドレスの学習がディセーブルになっています。この場合は、重大度 4 の Syslog メッセージ、STM_LEARNING_OVERLOAD が受信されています。

解決方法

120 秒待機した後、学習が自動的にイネーブルになります。

MAC アドレスが学習されない

スイッチによって MAC アドレスが学習されません。これが起こると、MAC アドレスは MAC テーブルに登録されません。

考えられる原因

ループの検出が原因で、MAC アドレスの学習がディセーブルになっています。この場合は、重大度 2 の Syslog メッセージ、STM_LOOP_DETECT が受信されています。

解決方法

180 秒待機した後、学習が自動的にイネーブルになります。重大度 2 の Syslog メッセージ、STM_LEARNING_RE_ENABLE が受信されます。

考えられる原因

MAC アドレス テーブルがいっぱいになっています。この場合は、重大度 2 の Syslog メッセージ、STM_LIMIT_REACHED が受信されています。

解決方法

180 秒待機した後、MAC テーブルがフラッシュされ、学習が自動的にイネーブルになります。あるいは、一部の MAC エントリの期限が切れて学習済みエントリの総数が 1500 より少なくなるまで待つか、「clear mac address-table dynamic [address <mac>]」コマンドを実行してエントリをクリアします。こうすると、新しい MAC エントリを学習するための空き領域が作成されます。重大度 2 の Syslog メッセージ、STM_LEARNING_RE_ENABLE が受信されます。

考えられる原因

学習の過負荷が原因で（つまり、新しいアドレスが短時間であまりにも多すぎたため）、MAC アドレスの学習がディセーブルになっています。この場合は、重大度 4 の Syslog メッセージ、STM_LEARNING_OVERLOAD が受信されています。

解決方法

120 秒待機した後、学習が自動的にイネーブルになります。

考えられる原因

着信データ トラフィック用の出力パスが設定されていません。スイッチから発信されるデータのパスがない場合、そのデータ ストリームから MAC アドレスは学習されません。

解決方法

データの送出パスを設定します。

たとえば、データが着信するインターフェイスを除くすべてのインターフェイスで VLAN がイネーブルになっていない場合があります。あるいは、送出インターフェイスがダウンしている場合もあります。この場合は、それらのインターフェイスをアップする必要があります。

VPC セットアップでのトラフィック フラッディング

VPC シナリオの下でデータが転送されず、代わりにフラッディングされます。

考えられる原因

MAC アドレスが 1 台のスイッチのみで学習されています。通常、この状況は VPC ピアとの MAC アドレスの同期に関するバグです。

解決方法

MAC アドレスが学習されたスイッチから MAC アドレスをクリアします。これにより、MAC アドレスの新しい学習と VPC スイッチ間での MAC アドレスの同期が行われます。

スパニング ツリー プロトコル

メッセージ「BPDUGuard errDisable」で HIF がダウンする

メッセージ「BPDUGuard errDisable」に伴って HIF がダウンします。

考えられる原因

デフォルトでは、HIF は BPDU ガードがイネーブルになった STP エッジ モードになります。つまり、HIF はホストまたは非スイッチング デバイスに接続するよう想定されています。HIF が BPDU を送信する非ホスト デバイスまたはスイッチに接続している場合、その HIF は BPDU の受信時にエラー ディセーブルになります。

解決方法

HIF およびピア接続デバイスで BPDUfilter をイネーブルにします。このフィルタをイネーブルにすると、HIF は BPDU を送信または受信しません。次のコマンドを使用して、ポートの STP ポート ステートの詳細を確認します。

- 「show spanning-tree interface <id> detail」
- 「show spanning-tree interface <id>」

スイッチで FWM-2-STM_LOOP_DETECT が検出され、動的学習がディセーブルになる

スイッチで FWM-2-STM_LOOP_DETECT が検出されると、動的学習がディセーブルになります。

考えられる原因

- 不適切な STP ポート ステートのコンバージェンスが原因で、MAC アドレスが移動しています。
- STP ステートがコンバージされて正しい状態にあるときにデータの送信元がすべてのスイッチを物理的に横断していることが原因で、MAC アドレスが移動しています。

次のコマンドを使用して、スイッチの VLAN 上の STP ポート ステートを確認します。

- 「show spanning-tree」
- 「show spanning-tree vlan <id>」

解決方法

- 正しい STP コンバージェンスを確認し、関係図内のすべてのスイッチで STP ポートステートをチェックします。また、競合がないこと、および不適切なポートステートがないことも確認します。
- 物理的に移動しているデータ フレームの送信元が特定された場合は、高速な連続的移動を停止するよう送信元を制御します。
- デフォルトでは、動的学習は 180 秒後に再開します。その時点で、すべての STP 競合または不整合は解決されます。

STP ブロッキング ステート「BLK*(Type_Inc)」でポートがスタックしている

STP ブロッキング ステート「BLK*(Type_Inc)」でポートがスタックしています。

考えられる原因

アクセス ポートが相手側のトランク ポートに接続するときに、アクセス ポートでタイプが一致していない可能性があります。リンクに不適切な設定があることを示すため、そのポートは BLK*(Type_Inc) になります。次のコマンドを使用して、ポートの STP ポート ステートの詳細を確認します。

- 「show spanning-tree interface <id> detail」
- 「show spanning-tree interface <id>」

解決方法

リンクの両端（ポート）で設定されている switchport モードを確認します。両者が同じモードになるようにします。両方をアクセス モードまたはトランク モードにする必要があります。モードが同期したら、ポートは不一致状態から正常な状態に移行します。

STP ブロッキング ステート「BLK*(PVID_Inc)」でポートがスタックしている

STP ブロッキング ステート「BLK*(PVID_Inc)」でポートがスタックしています。

考えられる原因

トランク リンク上でネイティブ VLAN の不一致があるときに、PVID が一致していない可能性があります。これが起こると、ポート ステートは「BLK* (PVID_Inc)」になります。次のコマンドを使用して、ポートの STP ポート ステートの詳細を確認します。

- 「show spanning-tree interface <id> detail」
- 「show spanning-tree interface <id>」

解決方法

リンクの両端（ポート）で設定されているネイティブ VLAN を確認します。両者が同じネイティブ VLAN を持つようにします。ネイティブ VLAN が同期したら、ポートは不一致状態から正常な状態に移行します。

STP ブロッキング ステート「BLK*(Loop_Inc)」でポートがスタックしている

STP ブロッキング ステート「BLK*(Loop_Inc)」でポートがスタックしています。

考えられる原因

この状況は、ポートでループガードが設定されていて、ポートで BPDU の受信が停止したときに起こります。これは単方向リンク障害が発生したときにループを防止する働きがあります。ただし、そのポートは「BLK* (Loop_Inc)」ステートになります。次のコマンドを使用して、ポートの STP ポート ステートの詳細を確認します。

- 「show spanning-tree interface <id> detail」
- 「show spanning-tree interface <id>」

解決方法

リンクの両端（ポート）で設定されているネイティブ VLAN を確認します。両者が同じネイティブ VLAN を持つようにします。ネイティブ VLAN が同期したら、ポートは不一致状態から正常な状態に移行します。

マルチキャスト

IGMP 加入の送信元 MAC アドレスが学習される

この状況では、IGMP 加入の送信元 MAC アドレスが学習されます。しかし、MAC アドレス空間を節約するため、スイッチでは通常、IGMP 加入の送信元 MAC アドレスは学習されません。

考えられる原因

加入の受信と ISSU の実行が同時に行われるとこの状況が起こる場合があります。

解決方法

加入が停止した場合、MAC アドレスは期限切れになります。あるいは、「clear mac address-table dynamic mac <mac>」コマンドを使用して明示的に MAC アドレスをクリアすることもできます。

マルチキャスト データ トラフィックがホストで受信されない

ホストでマルチキャスト データ トラフィックが受信されません。

考えられる原因

マルチキャストへの加入が登録されていません。

解決方法

- ホスト アプリケーションから加入が送信されていることを確認します。
- 「show vlan id <vlan>」コマンドを使用して、加入が送信されている VLAN にスイッチ ポートが設定されているかどうかを確認します。
- 「show vlan id <vlan>」コマンドを使用して、該当する VLAN がアクティブかどうかを確認します。
- 「show spanning-tree vlan <vlan>」コマンドを使用して、スイッチ ポートが STP フォワーディング ステートにあるかどうかを確認します。

ホストがグループに登録されているのにマルチキャスト データ トラフィックが受信されない

ホストがグループに登録されているのにマルチキャスト データ トラフィックが受信されません。

考えられる原因

IGMP プロセスと FWM プロセス間の通信にバグがある可能性があります。

次のコマンドの出力を調べます。

- 「show ip igmp snooping groups vlan 1001」
- 「show mac address-table multicast vlan 1001 igmp-snooping」
- 「show platform fwm info vlan 1001 all_macgs verbose」

解決方法

ホスト インターフェイスで「shut/no-shut」操作を実行し、加入をもう一度送信します。

VPC セットアップでマルチキャスト トラフィックがフラッディングする

VPC セットアップでマルチキャスト トラフィックがフラッディングします。

考えられる原因

いずれかのスイッチで IGMP スヌーピングがディセーブルになっています。

解決方法

両方のスイッチで IGMP スヌーピングをイネーブルにします。

（注）　リンク ローカル IP アドレス（つまり、224.0.0.X）のグループは作成されません。

VLAN

Nexus 5000 に VTP サーバを実行しているスイッチと同じ VLAN がない

Nexus 5000 の VLAN が、VTP サーバを実行しているスイッチの VLAN と同じではありません。

考えられる原因

Nexus 5000 では現在、透過モードの VTP のみがサポートされています（4.2(1)N1(1) 以降のリリース）。

解決方法

この状況は、VLAN をローカルに設定する必要があることを示します。ただし、次のコマンドを使用すると、VTP クライアントとサーバが Nexus 5000 を通じて通信できるようになります。

```
switch(config)# feature vtp
switch(config)# vtp mode transparent
switch(config)# exit
switch# show vtp status
```

VLAN が作成できない

VLAN が作成できません。

考えられる原因

内部 VLAN 範囲が使用されています。

解決方法

内部使用のために予約されていない VLAN 番号を使用します。

（注）　3968 ～ 4047 の VLAN 番号は内部使用のために予約されています。

例：

```
switch(config)# vlan ?
  <1-3967,4048-4093>  VLAN ID 1-4094 or range(s): 1-5, 10 or 2-5,7-19
```

インターフェイス VLAN がダウンしている

インターフェイス VLAN がダウンしています。

考えられる原因

VLAN が作成されていません。

解決方法

VLAN <###> がまだ作成されていなくても、NX-OS では「interface vlan <###>」の設定が許可されます。その結果、「interface vlan <###>」はアップしません。「show vlan」コマンドを使用して、VLAN <###> が存在するかどうかを確認します。存在しない場合は、「vlan <###>」コマンドを使用して VLAN を作成します。VLAN を作成した後、アップするためにインターフェイス VLAN をバウンスする必要があります。

例：

```
switch(config)# int vlan 600
switch(config-if)# no shut
switch(config-if)# sh int vlan 600 brief

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
--------------------------------------------------------------------------------
Vlan600   --                                      down   other
switch(config)# show vlan id 600
VLAN 600 not found in current VLAN database
switch(config-if)# vlan 600
switch(config)# show vlan id 600

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
600  VLAN0600                          active    Po1, Po11, Po30, Po31
switch(config-if)# int vlan 600
switch(config-if)# shut
switch(config-if)# no shut
switch(config-if)# show int vlan 600 brief

--------------------------------------------------------------------------------
Interface Secondary VLAN(Type)                    Status Reason
```

```
--------------------------------------------------------------------------------
Vlan600   --                                      up      --
```

ポートにアクセスするようにインターフェイスを設定しても VLAN <###> を通過できない

VLAN <###> を許可するためにインターフェイスをポートにアクセスするよう設定しても、VLAN <###> を通過できません。

考えられる原因

VLAN が作成されていません。

解決方法

NX-OS では、インターフェイスに対して「switchport access vlan <###>」コマンドを実行しても、VLAN <###> は自動的に作成されません。「vlan <###>」コマンドを使用して VLAN <###> を明示的に作成する必要があります。「show vlan」コマンドを使用して、VLAN <###> が存在するかどうかを確認します。存在しない場合は、「vlan <###>」コマンドを使用して VLAN を作成します。

VLAN が作成できない

VLAN が作成できません。

考えられる原因

VLAN リソースがすべて使用されています。

解決方法

Nexus 5000 では、アクティブな VLAN/VSAN の最大数はスイッチあたり 512 です（VSAN 用に 31、残りは VLAN 用）。「show resource vlan」コマンドを使用して、使用可能な VLAN の数を確認します。

例：

```
switch(config)# show resource vlan

     Resource               Min       Max      Used    Unused     Avail
    -----------            -----     -----    ------  --------   -------
     vlan                16       512        25         0       487
```

SVI が作成できない

SVI が作成できません。

考えられる原因

「interface-vlan」機能がイネーブルになっていません。

解決方法

SVI を設定する前に、「interface-vlan」機能をイネーブルにする必要があります。「show feature」コマンドを使用して、イネーブルになっている機能を確認します。

例：

```
switch(config)# feature interface-vlan
switch(config)# show feature
```

```
Feature Name          Instance  State
--------------------  --------  --------
tacacs                1         disabled
lacp                  1         enabled
interface-vlan        1         enabled
private-vlan          1         enabled
udld                  1         enabled
vpc                   1         enabled
fcoe                  1         disabled
fex                   1         enabled
```

プライベート VLAN（PVLAN）が作成できない

プライベート VLAN（PVLAN）が作成できません。

考えられる原因

「private-vlan」機能がイネーブルになっていません。

解決方法

PVLAN を設定する前に、「private-vlan」機能をイネーブルにする必要があります。そうすると、PVLAN コマンドが使用可能になります。「show feature」コマンドを使用して、イネーブルになっている機能を確認します。

例：

```
switch(config)# feature private-vlan
switch(config)# show feature
Feature Name          Instance  State
--------------------  --------  --------
tacacs                1         disabled
lacp                  1         enabled
interface-vlan        1         enabled
private-vlan          1         enabled
udld                  1         enabled
vpc                   1         enabled
fcoe                  1         disabled
fex                   1         enabled
```

レジスタとカウンタ

ドロップの識別

Nexus 5000 でフレームがドロップされるときは論理的かつ物理的な原因があります。また、スイッチ アーキテクチャのカットスルー特性のためにフレームをドロップできない場合もあります。ドロップする必要があるフレームがカットスルー パスで切り替えられている場合、唯一のオプションはイーサネット Frame Check Sequence（FCS; フレーム チェック シーケンス）をストンプすることです。フレームをストンプするには、CRC チェックを通過しない既知の値に FCS を設定します。こうすると、このフレームのパスの後の方で後続の CRC チェックが失敗します。これにより、ダウンストリームのストアアンドフォワード デバイスまたはホストがこのフレームをドロップできます。

（注）　フレームが 10 Gb/秒インターフェイスで受信されたとき、そのフレームはカットスルー パスにあるものと見なされます。

次の出力例は、特定のインターフェイスで見られたすべての廃棄とドロップ（キューイング ドロップを除く）を示します。キューイング ドロップは想定どおりの動作である場合があり、エラーの結果生じることもあります（ドロップは廃棄よりも一般的です）。

例：

```
switch# show platform fwm info pif ethernet 1/1 ...
Eth1/1 pd: tx stats: bytes 19765995 frames 213263 discard 0 drop 0
Eth1/1 pd: rx stats: bytes 388957 frames 4232 discard 0 drop 126
```

一部のコマンドでは、ポートが存在するチップを知っておく必要があります。

次の例では、チップの名称は「Gatos」です。この例は、どの Gatos とどの Gatos ポートがイーサネット 1/1 に関連付けられているかを示しています。

```
switch# show hardware internal gatos port ethernet 1/1 | include
instance|mac
         gatos instance     : 7 <- Gatos 7
         mac port           : 2 <- Port 2
         fw_instance        : 2
```

想定されたドロップ/論理的ドロップ

通常運用時、Nexus 5000 は論理的帰結に基づいて転送できないフレームに遭遇します。

たとえば、特定のインターフェイスで MAC アドレスを学習し、そのインターフェイスで受信したトラフィックが宛先としてその送信元インターフェイス上の MAC アドレスを持つ場合、このフレームは転送できません。これは既知のアドレスであり、したがってフラッディングできず、着信インターフェイスからトラフィックは送出できません。これはレイヤ 2 トポロジのループを回避するための要件です。

入力ポートが VLAN 内の唯一のポートである場合は、次の例に示すエラー カウンタが増加します。

例（前の例と同じ Gatos インスタンス）：

```
switch# show platform fwm info gatos-errors 7
Printing non zero Gatos error registers:
DROP_SRC_MASK_TO_NULL     9
```

（注）　「show platform fwm info gatos-errors」コマンドは、ある特定のドロップについてカウンタを 3 回増加させます。

その他の想定されたドロップ

ドロップ	説明
VLAN_MASK_TO_NULL	CPU インターフェイス宛てのトラフィック。 実際には VLAN ではありません。

ドロップ	説明
DROP_NO_FABRIC_SELECTED	VLAN_MASK_TO_NULL とともに増加します。
DROP_INGRESS_ACL	アクセスリストがフレームと一致した場合に増加します。 ACL が適用されていない場合には、NX-OS を DoS 攻撃から守るためにハードウェアでレート制限がイネーブルにされている場合に大量の CPU 宛てトラフィックが受信されると、このカウンタが増加します。

キューがいっぱいになった

キューがいっぱいになったときは、入力インターフェイス上の個々のキューで廃棄を増やす必要があります。

例：

```
switch# show queuing interface e1/1
Ethernet1/1 queuing information:
   TX Queuing
     qos-group  sched-type  oper-bandwidth
         0       WRR             50
         1       WRR             50

   RX Queuing
     qos-group 0
     q-size: 243200, HW MTU: 1600 (1500 configured)
     drop-type: drop, xon: 0, xoff: 1520
     Statistics:
         Pkts received over the port             : 0
         Ucast pkts sent to the cross-bar        : 0
         Mcast pkts sent to the cross-bar        : 0
         Ucast pkts received from the cross-bar  : 0
         Pkts sent to the port                   : 0
     <b>    Pkts discarded on ingress               : 0 </b>
         Per-priority-pause status               : Rx (Inactive), Tx
(Inactive)

     qos-group 1
     q-size: 76800, HW MTU: 2240 (2158 configured)
     drop-type: no-drop, xon: 128, xoff: 240
     Statistics:
         Pkts received over the port             : 0
         Ucast pkts sent to the cross-bar        : 0
         Mcast pkts sent to the cross-bar        : 0
         Ucast pkts received from the cross-bar  : 0
         Pkts sent to the port                   : 0
     <b>   Pkts discarded on ingress               : 0 </b>
         Per-priority-pause status               : Rx (Inactive), Tx
(Inactive)

   Total Multicast crossbar statistics:
     Mcast pkts received from the cross-bar      : 0
```

MTU 違反

Nexus 5000 は 10 Gb/秒ではカットスルー スイッチです。これは、MTU のチェックはできるものの、長さがわかるときにはすでにフレームの送信が開始されていることを意味します。したがって、フレームはドロップできません。このようなフレームは MTU に達した後に切り捨てられ、CRC 値がストンプされます。入力インターフェイスでは Rx Jumbo が増加し、出力インターフェイスでは Tx CRC と Tx Jumbo が増加します。

- 「show interface」コマンドまたは「show hardware internal gatos port e1/1 counters rx」コマンドでジャンボ フレームが示される場合、これはそれらのフレームがドロップされたことを意味するものではありません。ジャンボ フレームとは単に、受信または送信された 1500 バイトを超えるイーサネット フレームのことです。
- 「show queuing interface ex/y」コマンドは、現在の（クラスごとの）MTU の設定値を示します。
- MTU 違反に起因するドロップを確認するには、「show hardware internal gatos counters interrupt match mtu*」コマンドを使用します。
- 「show hardware internal gatos port ethernet 1/1 | include instance|mac」コマンドによって出力される、Gatos 番号と fw_instance に一致するカウンタは、MTU 違反が発生してフレームがストンプされたことを示す指標です。

CRC エラーの処理

カットスルー ポート上の FCS で CRC エラーが発生した場合は、「show interface」の Rx CRC カウンタが増加します。ただし、FCS はワイヤ上のイーサネット フレームの最後にあるため、CRC エラーのフレームはドロップできません。

出力インターフェイスの Tx CRC エラーが増加し、パス上の次のデバイスに伝播します。

Nexus 5000 が CRC を伝播または生成しているかどうかを確認するには、「show hardware internal gatos counters interrupt match stomp」コマンドを使用します。

- ストンプ値が存在する場合は、そのインターフェイス上に一致する CRC 値があります。
- Rx CRC 値が存在する場合は、すでにエラーのある状態でスイッチポートに入ってきたことがわかります。接続されているデバイスに移動し、エラーをさかのぼって追跡できます。

CHAPTER 4

QoS の問題のトラブルシューティング

Cisco Nexus 5000 シリーズの NX-OS Quality of Service（QoS）は、ネットワークを通じた最も望ましいトラフィック フローを提供するために使用されます。QoS はポリシーとフロー制御を使用することで、ネットワーク トラフィックを分類し、トラフィック フローをポリシングおよび優先順位付けして、輻輳を回避します。

この章では、Cisco Nexus 5000 シリーズ スイッチの QoS で起こり得る問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。

ポリシー マップ

Nexus 5000 の QoS の実装は、Cisco モジュラ QoS CLI モデルに従います。QoS の設定には次の 3 つの手順が関係します。

- クラスマップを定義する。
- ポリシーマップを作成し、各クラスマップに対して実行するアクションを定義する。
- ポリシーマップを適用する。

Nexus 5000 には、次の 3 つのタイプのポリシーマップが実装されています。

- policy-map type qos
- policy-map type queuing
- policy-map type network-qos

また、Nexus 5000 には「システム QoS」と呼ばれる QoS の新しい設定コンテキストが導入されています。「システム QoS」コンテキストの下で適用されたポリシーマップはスイッチ全体に適用されます。

次の表に、これら 3 つのタイプのポリシーマップの機能と付加する箇所をまとめます。

表 4-1　ポリシー マップのタイプ

ポリシー タイプ	機能	付加する箇所
QoS	• トラフィック分類を定義します。	• システム QoS • 入力インターフェイス
キューイング	• 完全優先キュー • Deficit Weight Round Robin	• システム QoS • 出力インターフェイス • 入力インターフェイス
ネットワーク QoS	• フロー制御メカニズム（PAUSE またはテール ドロップ）を定義します。 • サービス クラスごとの MTU • キュー サイズ • マーキング	• システム QoS

基本プロセスは次のとおりです。まず、着信パケットが「policy-map type qos」によって定義された QoS 分類ルールと比較されます。これにより、パケットが 8 つの QoS グループのいずれかに分類されます。

次に、ネットワーク QoS ポリシーとキューイング ポリシーがパケットに適用されます。キューイング ポリシーとネットワーク QoS ポリシーは、各 QoS グループに属するパケット用の実際の QoS パラメータを定義します。

（注）
- キューイング ポリシーとネットワーク QoS ポリシーは、実際のパケット ヘッダーではなく（「policy-map type qos」によって識別された）QoS グループと一致します。
- システム QoS コンテキストの配下とインターフェイス レベルで同じタイプのサービス ポリシーが適用されている場合は、インターフェイス レベルのサービス ポリシーが優先されます。
- 入力インターフェイスの下で適用されたキューイング ポリシーはローカルには適用されません。キューイング ポリシーは、DCBX プロトコルを使用したピア間で交換される各サービス クラスに対する帯域幅の割り当てです。

不適切な設定

2300 バイトよりも大きいフレーム サイズがスイッチを通過できない

「class-default」でジャンボ MTU が設定されているにもかかわらず、2300 バイトよりも大きいフレーム サイズが Nexus 5000 スイッチおよび Nexus 2000 FEX を通過できません。

考えられる原因

CoS 値が既存の MTU 値と衝突している可能性があります。

解決方法

CoS 7 は、Nexus 5000 スイッチと Nexus 2000 FEX 間のトラフィックを制御するために内部で使用されます。CoS 7 を持つトラフィックの MTU 値は固定値に設定されます。着信トラフィックが CoS 7 でマークされていることを確認する必要があります。この制限を回避するには、7 以外の任意の CoS 値を使用します。

ジャンボ MTU が設定されているとき、「class-default」値の MTU が 1500 である

「network-qos policy-map」の設定によって「class-default」がジャンボ MTU に設定されているとき、「show queuing interface」コマンドを実行すると「class-default」の MTU が 1500 と表示されます。

考えられる原因

アップグレード後、不適切なスタートアップ コンフィギュレーションが存在する可能性があります。

解決方法

スイッチを 4.2(1)N1(1) リリースにアップグレードした場合は、「write erase」コマンドを使用してスタートアップ コンフィギュレーションを削除したことを確認します。コンフィギュレーションは削除操作の前に別のファイル名に保存できます。

Nexus 5000 スイッチが空のコンフィギュレーションで起動したら、元のコンフィギュレーションを再び適用します。telnet または ssh を使用している場合は、Nexus 5000 への接続が失われる場合があることに注意してください。この手順を行う際はコンソールを使用することを推奨します。

Nexus 2148、Nexus 2232、および Nexus 2248 でトラフィックのキューイングまたは優先順位付けが正しく行われない

3 つのタイプのポリシーマップ（QoS、ネットワーク QoS、キューイング）をすべて設定した後、Nexus 2148、Nexus 2232、および Nexus 2248 スイッチでトラフィックのキューイングまたは優先順位付けが正しく行われません。

考えられる原因

Nexus 2148、Nexus 2232、および Nexus 2248 FEX は、CoS ベースのトラフィック分類のみをサポートします。システム QoS の下で設定された QoS サービス ポリシー タイプは、一致基準がすべて「match cos」の場合にのみ、Nexus 5000 から FEX に読み込まれます。その他の match 句（「match dscp」や「match ip access-group」など）が QoS ポリシーマップに存在する場合、FEX はそのサービス ポリシーを受け入れません。その結果、すべてのトラフィックがデフォルト キューに配置されます。

（注）　キューが適切に作成されているかどうかを確認するには、「show queuing interface」コマンドを使用します。

解決方法

CoS 値でマークされていない（サーバからネットワークへの）入力トラフィックは、FEX 上でデフォルト キューに配置されます。そのトラフィックが Nexus 5000 で受信されると、設定されたルールに基づいて分類され、適切なキューに配置されます。

（Nexus5000 から FEX を介してサーバに至る）出力トラフィックでは、FEX がトラフィックを適切に分類してキューに配置できるように、Nexus 5000 で CoS 値によってトラフィックをマークすることを推奨します。

次に、Nexus 5000 および Nexus 2232/Nexus 2248 で、トラフィックを分類してトラフィックのタイプごとに適切な帯域幅を設定する全コンフィギュレーションの例を示します。この例を適用できるのは、Nexus 5000 および Nexus 2248 のみです。Nexus 2148 にはユーザ データ用のキューが 2 つしかないため、Nexus 2148 のコンフィギュレーションは少し異なります。Nexus 2232/Nexus 2248 にはユーザ データ用のハードウェア キューが 6 個あり、これは Nexus 5000 と同じです。

例：

```
//class-map for global qos policy-map, which will be used to create CoS-queue mapping.//
class-map type qos voice-global
match cos 5
class-map type qos critical-global
match cos 6
class-map type qos scavenger-global
match cos 1
class-map type qos video-signal-global
match cos 4

//This qos policy-map will be attached under “system qos”. It will be downloaded to 2248
to create CoS to queue mapping.//
policy-map type qos classify-5020-global
class voice-global
set qos-group 5
class video-signal-global
set qos-group 4
class critical-global
set qos-group 3
class scavenger-global
set qos-group 2
class-map type qos Video
match dscp 34
class-map type qos Voice
match dscp 40,46
class-map type qos Control
match dscp 48,56
class-map type qos BulkData
match dscp 10
class-map type qos Scavenger
match dscp 8
class-map type qos Signalling
match dscp 24,26
class-map type qos CriticalData
match dscp 18

//This qos policy-map will be applied under all N5k and 2248 interfaces to classify all
incoming traffic based on DSCP marking. Please note that even the policy-map will be
applied under Nexus 2248 interfaces the traffic will be classified on N5k//
policy-map type qos Classify-5020
class Voice
set qos-group 5
class CriticalData
set qos-group 3
class Control
set qos-group 3
class Video
set qos-group 4
class Signalling
set qos-group 4
class Scavenger
set qos-group 2
class-map type network-qos Voice
match qos-group 5
class-map type network-qos Critical
```

```
match qos-group 3
class-map type network-qos Scavenger
match qos-group 2
class-map type network-qos Video-Signalling
match qos-group 4

//This policy-map type network-qos will be applied under "system qos" to define the MTU,
marking and queue-limit(not configured here).//
policy-map type network-qos NetworkQoS-5020
class type network-qos Voice
set cos 5
class type network-qos Video-Signalling
set cos 4
mtu 9216
class type network-qos Scavenger
set cos 1
mtu 9216
class type network-qos Critical
set cos 6
mtu 9216
class type network-qos class-default
mtu 9216
class-map type queuing Voice
match qos-group 5
class-map type queuing Critical
match qos-group 3
class-map type queuing Scavenger
match qos-group 2
class-map type queuing Video-Signalling
match qos-group 4

//The queuing interface will be applied under "system qos" to define the priority queue
and how bandwidth is shared among non-priority queues.//
policy-map type queuing Queue-5020
class type queuing Scavenger
bandwidth percent 1
class type queuing Voice
priority
class type queuing Critical
bandwidth percent 6
class type queuing Video-Signalling
bandwidth percent 20
class type queuing class-fcoe
bandwidth percent 0
class type queuing class-default
bandwidth percent 73

//The input queuing policy determines how bandwidth are shared for FEX uplink in the
direction from FEX to N5k. The output queueing policy determines the bandwidth allocation
for both N5k interfaces and FEX host interfaces.//
system qos
service-policy type qos input classify-5020-global
service-policy type network-qos NetworkQoS-5020
service-policy type queuing input Queue-5020
service-policy type queuing output Queue-5020

//Apply service-policy type qos under physical interface in order to classify traffic
based on DSCP. Please note that for portchannel member the service-policy needs to be
configured under interface port-channel.//
interface eth1/1-40
service-policy type qos input Classify-5020
interface eth100/1/1-48
service-policy type qos input Classify-5020
```

「show queuing interface」コマンドを使用して、FEX インターフェイスで CoS とキューのマッピングが適切に設定されているかどうかを確認できます。また、帯域幅と MTU の設定を確認することもできます。

この同じコマンドを使用して、Nexus 5000 インターフェイスの QoS 設定を確認できます。

次に、上記のコンフィギュレーションを適用したときの Nexus 2248 インターフェイスの「show queuing interface」コマンドの出力を示します。

```
switch# sh queuing interface ethernet 100/1/1
Ethernet100/1/1 queuing information:
  Input buffer allocation:
  Qos-group: 0  2  3  4  5  (shared)
  frh: 2
  drop-type: drop
  cos: 0 1 2 3 4 5 6
xon       xoff      buffer-size
  ------+---------+-----------
  21760     26880     48640
Queueing:
  queue qos-group cos            priority  bandwidth mtu
  -----+----------+------------+-----------+--------------+------
  2        0            0 2 3          WRR         73      9280
  4        2            1              WRR          1      9280
  5        3            6              WRR          6      9280
  6        4            4              WRR         20      9280
  7        5            5              PRI          0      1600
Queue limit: 64000 bytes

  Queue Statistics:
  queue  rx              tx
  ------+-------------+---------------
  2      113822539041    1
  4      0               0
  5      0               0
  6      417659797       0
  7      0               0
Port Statistics:
  rx drop         rx mcast drop   rx error        tx drop
  ------------+----------------+---------------+---------------
  0               0               0               0

  Priority-flow-control enabled: no
  Flow-control status:
  cos     qos-group   rx pause  tx pause  masked rx pause
  -------+-----------+---------+---------+---------------
  0              0    xon       xon       xon
  1              2    xon       xon       xon
  2              0    xon       xon       xon
  3              0    xon       xon       xon
  4              4    xon       xon       xon
  5              5    xon       xon       xon
  6              3    xon       xon       xon
  7            n/a    xon       xon       xon
switch#
```

Nexus 2148 には入力方向と出力方向の両方に 2 つのキューがあります。一方のキューは no-drop システム クラスにマップされ、もう一方のキューは drop システム クラスにマップされます。入力方向では、Weight Round Robin（WRR; 重み付けラウンド ロビン）を使用して 2 つのキューがスケジュールされます。出力方向では、no-drop システム クラスのキューがプライオリティ キューになります。

2 つのキューのトラフィックを分離するためには、ユーザが no-drop システム クラスを作成する必要があります。Nexus 5000 で作成された no-drop システム クラスはすべて、Nexus 2148 上の no-drop キューにマップされます。

FEX 出力方向で Nexus 2148 が音声をプライオリティ キューに配置できるようにするには、ネットワーク QoS に「pause no-drop」コマンドを追加します。

例：

```
policy-map type network-qos NetworkQoS-5020
  class type network-qos Voice
    set cos 5
    pause no-drop
  class type network-qos Video-Signalling
    set cos 4
    mtu 9216
  class type network-qos Scavenger
    set cos 1
    mtu 9216
  class type network-qos Critical
    set cos 6
    mtu 9216
  class type network-qos class-default
    mtu 9216
```

このコンフィギュレーションは着信音声トラフィックを DSCP に基づいて分類し、音声トラフィックを CoS 5 にマークします。Nexus 2148 は、FEX 出力方向で音声トラフィックをプライオリティ キューに割り当てます。

次に、上記のコンフィギュレーションを適用したときの Nexus 2148 の「show queuing interface」コマンドの出力例を示します。

例：

```
switch# sh queuing interface ethernet 199/1/1
Ethernet199/1/1 queuing information:
  Input buffer allocation:
  Qos-group: 0  2  3  4  (shared)
  frh: 3
  drop-type: drop
  cos: 0 1 2 3 4 6 7
  xon       xoff      buffer-size
  ---------+---------+-----------
  16640     33280     56320

  Qos-group: 5
  frh: 2
  drop-type: no-drop
  cos: 5
  xon       xoff      buffer-size
  ---------+---------+-----------
  8960      19200     34560

  Queueing:
  queue    qos-group    cos            priority  bandwidth mtu
  ------+------------+--------------+---------+----------+----
3        0 2 3 4      0 1 2 3 4 6     WRR       100       9280
  2        5            5               PRI         0      1600

  Buffer threshold: 271360 bytes
  Queue limit: Disabled

  Queue Statistics:
  queue  rx
```

```
  ------+---------------
  3      241439087
  2      0

  Port Statistics:
  tx queue drop
  ---------------
  0

  Priority-flow-control enabled: no
  Flow-control status:
  cos     qos-group   rx pause  tx pause  masked rx pause
  -------+-----------+---------+---------+---------------
  0              0    xon       xon       xon
  1              2    xon       xon       xon
  2              0    xon       xon       xon
  3              0    xon       xon       xon
  4              4    xon       xon       xon
  5              5    xon       xon       xon
  6              3    xon       xon       xon
  7            n/a    xon       xon       xon
switch#
```

PFC

バック ツー バックの Nexus 5000 スイッチ リンクでリンク ポーズ（フロー制御）がイネーブルになっていない

バック ツー バックの Nexus 5000 スイッチ リンクでリンク ポーズ（フロー制御）がイネーブルになっていないときは、no-drop クラスでトラフィックを送信しながらパケットがドロップされます。

考えられる原因

ピア Nexus 5000 スイッチで DCBX による PFC TLV がサポートされている場合、「flowcontrol send on」と「flowcontrol receive on」を設定してもリンク ポーズはイネーブルになりません。そのインターフェイスで DCBX によって送信される PFC TLV をディセーブルにする必要があります。

確認するには次のいずれかのコマンドを使用します。

- 「show interface ethx/y flowcontrol」コマンドを使用して、動作ステートが「off」かどうかを確認します。
- 「show interface ethx/y priority-flow-control」コマンドを使用して、動作ステートが「on」かどうかを確認します。

解決方法

「interface ethx/y」の下で次のコマンドを設定して、バック ツー バックのスイッチ リンクで PFC ではなくリンク ポーズをイネーブルにします。

- 「no priority-flow-control mode on」
- 「flowcontrol receive on」
- 「flowcontrol send on」

複数のイーサネット クラスで「pause no-drop」をイネーブルにできない

複数のイーサネット クラスで pause「no-drop」をイネーブルにできません。

「pause no-drop」をイネーブルにしようとすると、次のエラーが発生して CLI コマンドが失敗します。

```
ERROR:   Module 1 returned status "Not enough buffer space available. Please change your
configuration and re-apply"
```

考えられる原因

Nexus 5000 でサポートされている no-drop クラスの最大数は 3 つです（FCoE を含む）。5 つのイーサネット クラスを作成する場合、5 つのイーサネット no-drop クラスのうち 2 つをイネーブルにするためのバッファが足りません。

no-drop をイネーブルにするための十分なバッファが存在しない場合は、エラーが発生します。

例：

```
class type network-qos s4
pause no-drop
ERROR:   Module 1 returned status "Not enough buffer space available. Please change your
configuration and re-apply"
```

解決方法

5 つのイーサネット クラスを作成する場合、5 つのイーサネット no-drop クラスのうち 2 つを設定するためのバッファの数が足りません。2 つのイーサネット クラスを削除し、残り 3 つのイーサネット クラス（class-default を含む）を設定する場合、2 つのイーサネット クラスについて no-drop をイネーブルにできます。

no-drop 設定を変更すると、VPC ピアリンクがダウンし、FEX がオフラインになる

QoS no-drop 設定を変更すると、VPC MCT ピアリンクがダウンし、FEX がオフラインになります。

考えられる原因

MTU やポーズなどのネットワーク QoS ポリシー パラメータはタイプ 1 パラメータとして扱われ、VPC プライマリ ノードとセカンダリ ノードの間で一致している必要があります。VPC プライマリ ノードとセカンダリ ノードの間で不一致が存在する場合、VPC ピアリンクはアップせず、FEX はオフラインになります。VPC のタイプ 1 整合性がチェックされるのは、cos ベース クラスの no-drop/MTU パラメータだけです。acl ベース クラスを設定した場合は、VPC の vtype 1 パラメータとしては扱われません。

確認するには次のいずれかのコマンドを使用します。

- 「show vpc brief」
- 「show vpc consistency-parameters global」

解決方法

VPC プライマリ ノードとセカンダリ ノードの間でほぼ同じ no-drop クラス コンフィギュレーションを設定します。nqos cos ベース クラスのパラメータで no-drop ポリシーの不一致があると、タイプ 1 の不整合が発生します。

class-ip-multicast で no-drop をイネーブルにしたとき、すべての CoS 値でポーズがイネーブルになる

class-ip-multicast クラスで no-drop をイネーブルにしたとき、プライオリティ フロー制御により、すべての CoS 値でポーズがイネーブルになります。

考えられる原因

class-ip-multicast クラスを作成して no-drop をイネーブルにしたとき、すべての CoS 値でポーズがイネーブルにされています。

確認するには次のコマンドを使用します。

「show interface ethx/y priority-flow-control」コマンドを使用して、VL ビットマップがすべての CoS 値に対してイネーブルになっている（ff）かどうかを確認します。

解決方法

次のコマンドを使用して、class-ip-multicast クラスの下ですべての CoS 値ではなく CoS 4 に対してのみ PFC がイネーブルになるようにします。

- 「Policy-map type network-qos system」
- 「Class type network-qos class-ip-multicast」
- 「Pause no-drop pfc-cos 4」

デフォルトの QoS 設定を持つ N2K-C2148T/N2K-C2248TP-1GE ベースの FEX で no-drop クラスが作成されない

デフォルトの QoS 設定を持つ N2K-C2148T/N2K-C2248TP-1GE ベースの FEX で no-drop クラスが作成されません。

N2K-C2248TP および N2K-C2148T 上のスイッチポートと HIF ポートで show queuing interface が異なります。

考えられる原因

N2K-C2148T および N2K-C2248TP-1GE ベースの FEX では FCoE がサポートされておらず、デフォルトの QoS 設定では no-drop クラスは作成されません。

確認するには次のコマンドを使用します（no-drop クラスについて確認します）。

「show queuing interface eth100/1/1」

解決方法

N2K-C2148T/N2K-C2248TP-1GE FEX でイーサネット no-drop クラスが必要な場合は、次のコマンドを使用してイーサネット no-drop クラスを作成する必要があります。

- 「Policy-map type network-qos no-drop」
- 「Class type network-qos class-0」
- 「Pause no-drop」

Nexus 5000 インターフェイスでリンク ポーズ（フロー制御）をイネーブルにする方法

別の Nexus 5000 インターフェイスに接続されたときは、「flowcontrol send on」と「flowcontrol receive on」を設定しても Nexus 5000 スイッチ ポート リンクで「flowcontrol on」はイネーブルになりません。

Nexus 5000 インターフェイスでリンク ポーズ（フロー制御）をイネーブルにする方法。

考えられる原因

Nexus 5000 インターフェイスでは、デフォルトで DCBX が実行されます。ピアで DCBX が実行されていない場合、そのインターフェイスではテールドロップが設定されます。

確認するには次のいずれかのコマンドを使用します。

- 「show interface ethx/y flowcontrol」コマンドを使用して、動作ステートが「off」かどうかを確認します。
- 「show interface ethx/y priority-flow-control」コマンドを使用して、動作ステートが「off」かどうかを確認します。

解決方法

interface ethx/y の下で次のコマンドを使用して、リンク ポーズをイネーブルにします。

- 「flowcontrol receive on」
- 「flowcontrol send on」

レジスタとカウンタ

次に、各種レジスタやカウンタにアクセスするコマンドを示します。

Nexus 5000 10G PFC

次のコマンドを使用します。

```
show hard in gatos asic <gatos_num> registers match mm_CFG_pause.$
```

Nexus 5000 1G ストーム制御

次のコマンドを使用します。

```
show plat fwm info lif eth1/1
show plat fwm info pif eth1/1
debug hardware internal gatos asic 0 dump-mem 0x3b9000 20
```

Nexus 5000 10G ストーム制御

次のコマンドを使用します。

```
show plat fwm info lif eth1/5
```

```
show plat fwm info pif eth1/5
debug hardware internal gatos asic 1 dump-mem 0x3b9000 20    <<< for port 2
```

Nexus 5000 ストーム制御カウンタ

次のコマンドを使用します。

```
show hardware internal gatos asic 1 counters rx_db 2 | grep storm
```

afm 関連の CLI コマンドとツール

コマンド	目的
「show platform afm info att br」	どの機能またはグループがどのインターフェイスに付加されているかを表示します。
「show platform afm info att global」	グローバル インターフェイスに付加された QoS ポリシー（「NP Policies」と出力されます）を含むポリシーの ID を表示します。
「show platform afm info att interface ethernet x/y」	インターフェイスまたは PC の QoS ポリシーを含むポリシーの ID を表示します。
「show platform afm info group id X asic Y」	特定の ASIC/GATOS 上の特定のグループの TCAM エントリを表示します。
「show platform afm info map-tbls」	ext-cos 対 qos-group、qos-group 対 int-cos、int-cos 対 class_id などの内部マッピング テーブルを表示します。

FEX qosctrl デバッグ コマンド

コマンド	目的
「show platform software qosctrl port 0 0 nif <0-48> [sat|switch]」	すべてのポートの PI 情報を表示します。 （ポート レベルのコンフィギュレーションがある場合に便利です）
「show platform software qosctrl port 0 0 hif <0-48> [sat|switch]」	すべてのポートの PI 情報を表示します。 （ポート レベルのコンフィギュレーションがある場合に便利です）
「show platform software qosctrl policy hif」	グローバルなネットワーク QoS とキューイングの設定を表示します。
「show platform software qosctrl global」	グローバルな PI レベルのコンフィギュレーション。
「show platform software qosctrl pss」	保存されている PSS 情報。

コマンド	目的
「show platform software qosctrl asic <mod> <asic>」	ASIC レベルごとのポートの詳細を表示します。
「show platform software qosctrl default port <mod> <asic>」	FEX ポートのデフォルト ポート設定を表示します。
「show platform software qosctrl port <mod> <asic> <port-type> <port>」	ポート レベルごとの PI および PD データ構造を表示します。

N2K-C2148T FEX カウンタ

（注）　MAC レベル トラフィックの統計情報とポーズ統計情報を表示する準備として、（FEX シェルで）次のコマンドを使用します。
- 「show plat soft fex info satport <fex-interface-id>」（RW6 の NIF の場合を除くマッピングのため）
- 「show plat soft redwood sts」
- 「show plat soft redwood ss」

コマンド	目的
「show platform software qosctrl port 0 6 hif 1 counters」	カウンタを表示します。
「show plat soft redwood rmon 6 nif0」	eth103/1/37 の NIF の MAC レベル トラフィックの統計情報とポーズ統計情報を表示します。
「show plat soft redwood rmon 6 hif5」	eth103/1/37 の iHIF の MAC レベル トラフィックの統計情報とポーズ統計情報を表示します。
「show plat soft redwood rmon 4 nif1」	eth103/1/37 の iNIF の MAC レベル トラフィックの統計情報とポーズ統計情報を表示します。
「show plat soft redwood rmon 4 hif5」	eth103/1/37 の HIF の MAC レベル トラフィックの統計情報とポーズ統計情報を表示します。
「show plat soft redwood ss」	HIF/NIF と SS とのマッピングを表示します。
「show plat soft redwood ss 4 3」	RW4 SS3 の統計情報を表示します（HIF4-7 から NIF0-3 までのホスト受信）。
「show plat soft redwood ss 4 2」	RW4 SS2 の統計情報を表示します（HIF0-3 から NIF0-3 までのホスト受信）。
「show plat soft redwood rate」	非ゼロ トラフィックの全体的な統計情報を表示します。
「show plat soft redwood rmon 6 cif0」	CIF から CPU へのトラフィックのデバッグに役立ちます。
「show plat soft qosctrl port 0 6 cif 0 counters」	CIF から CPU へのトラフィックのデバッグに役立ちます。

Nexus 5000 マルチキャスト最適化

次のコマンドを使用します。

「show plat fwm in mco-info」
「show plat fwm in vlan 1 all_macgs」

Nexus 5000 FCoE 分類

- FCoE インターフェイスでは、次のコマンドを使用します。

  「show plat fwm info pif ethernet 1/1 | grep gatos」
  「debug platform hardware peek lu 7 index 5 pifTable」

- FC インターフェイスでは、次のコマンドを使用します。
  （最初のコマンドは gatos 番号と fc 番号を取得するために使用します）

  「show platform fwm info pif fc <id>」
  「debug peek lu <gatos> index <fc num> pifTable」

Nexus 5000 MTU プログラミング

次のコマンドを使用します。

「show hardware internal gatos asic 0 registers match bm_port_CFG.*_max.*」

Nexus 5000 割り込み

次のコマンドを使用します。

「debug hardware internal gatos asic 0 clear-interrupt」
「show hardware internal gatos asic 0 interrupt」
「show hardware internal gatos event-history errors」

タグなし CoS

次のコマンドを使用します。

「sh platform afm info attachment interface eth3/1」
「sh system internal ipqos port-node eth3/1」

N2K-C2232P FEX でのバッファの使用とパケット ドロップのデバッグ

次のコマンドを使用します。

「show platform software qosctrl asic 0 0」

CHAPTER 5

SAN スイッチングの問題のトラブルシューティング

Storage Area Network（SAN; ストレージ エリア ネットワーク）は、サーバ用のデータ ストレージを提供するストレージ デバイスのネットワークです。

この章では、SAN と Cisco Nexus 5000 シリーズ スイッチで起こり得る問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。

概要

ストレージ ネットワークの問題で最もよく見られる症状は次の 2 つです。

- ホストから、ホストに割り当てられたストレージにアクセスできない。
- アプリケーションが、割り当てられたストレージにアクセスしようとした後、応答しない。

次の項目を確認することで、実施する手順と詳細な調査が必要なコンポーネントを特定できます。これらの項目はホスト、スイッチ、またはサブシステムのベンダーに依存しません。

次の項目を確認して、インストールのステータスを判別します。

- 新たにインストールしたシステムであるか、既存のシステムであるかを確認します（新しい SAN、ホスト、またはサブシステムであるか、既存のホストにエクスポートされた新しい LUN であるか）。
- これまでホストがそのストレージを認識していたかどうかを確認します。
- ホストがサブシステム内のいずれかの LUN を認識しているかどうかを確認します。
- 既存のアプリケーションの問題（遅い、遅延が長い、応答時間が極端に長い）を解決しようとしているのか、最近出現した問題であるかを確認します。
- アプリケーションで問題が発生する直前に、設定またはインフラストラクチャ全体にどのような変更を加えたかを確認します。

一般的な SAN のトラブルシューティング手順

ステップ 1　ファブリック内の問題に関する情報を収集します。
ステップ 2　スイッチとエンド デバイス間の物理接続を確認します。
ステップ 3　すべての SAN 要素についてファブリックへの登録を確認します。
ステップ 4　エンド デバイス（ストレージ サブシステムおよびサーバ）の設定を確認します。
ステップ 5　エンドツーエンドの接続とファブリックの設定を確認します。

NPV

NPV エッジ スイッチの NP アップリンク ポートが初期化ステートでスタックしている

コア NPIV スイッチに接続された NP アップリンク ポートがオンラインにならず、初期化ステートでスタックしています。

考えられる原因

コア スイッチで NPIV がイネーブルになっていない可能性があります。

例：

```
switch(config-if)# sh int fc2/2
fc2/2 is down (Initializing)
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:42:00:0d:ec:a4:3b:80
Admin port mode is NP, trunk mode is on
```

解決方法

- NPV 外部インターフェイスのステータスを確認します。
  コア スイッチで NPIV がイネーブルになっているかどうかを確認します。

  例：

  ```
  switch(config-if)# sh npv status
  npiv is disabled
  disruptive load balancing is disabled
  External Interfaces:
  ====================
  Interface: fc2/1, State: Failed(NPIV is not enabled in upstream switch)
  Interface: fc2/2, State: Failed(NPIV is not enabled in upstream switch)
  Interface: san-port-channel 200, State: Down
  ```

- NPIV がディセーブルの場合は、コア スイッチで NPIV をイネーブルにします。

  例：

  ```
  switch(config)# feature npiv
  ```

サーバ インターフェイスがアップせず、「NPV upstream port not available」メッセージが表示される

NPV エッジ スイッチに接続されたサーバ ポートがオンラインにならず、show interface コマンドを実行すると「NPV upstream port not available」のステータスが表示されます。

考えられる原因

NPV エッジ スイッチ上のアップストリーム NP_Port とダウンストリーム サーバ F_Port が同じ VSAN に属していない可能性があります。

例：

```
switch# sh int fc2/7
fc2/7 is down (NPV upstream port not available)
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:47:00:0d:ec:a4:3b:80
Admin port mode is F, trunk mode is off
snmp link state traps are enabled
Port vsan is 99
Receive data field Size is 2112
```

解決方法

- アップストリーム ポートとサーバ ポートの VSAN メンバーシップを確認します。

  例：

  ```
  switch# show vsan membership
  vsan 1 interfaces:
  fc2/1 fc2/2 fc2/3 fc2/4
  fc2/5 fc2/6 san-port-channel 200
  vsan 99 interfaces:
  fc2/7 fc2/8
  ```

- 上の例では、アップストリーム ポート（fc2/1-2）は VSAN 1 に属し、サーバ ポート（fc2/7-8）は VSAN 99 に属しています。
  NPV エッジ上の NP ポートと NPIV コア上の F ポートをサーバ ポートと同じ VSAN に移動します。

  例：

  ```
  switch(config)# vsan database
  switch(config-vsan-db)# vsan 99 interface fc2/1-2
  switch(config-if)# vsan database
  switch(config-vsan-db)# vsan 99 interface fc1/17-18
  Traffic on fc1/17 may be impacted. Do you want to continue? (y/n) y
  Traffic on fc1/18 may be impacted. Do you want to continue? (y/n) y
  ```

（注） あるいは、NPIV コア スイッチと NPV エッジ スイッチが F_Port トランキングに対応したスイッチである場合は、それが推奨されるコンフィギュレーションです。

NPV NP ポート間の不均等なロード バランシング

同じ VSAN のメンバーである NP アップストリーム ポートを調べると、ロード バランシングが不均等になっています。

考えられる原因

これは通常の状態で、N5000 Dee Why 4.2(1)N1 リリースよりも前のリリースで提供されているデフォルトの SID/DID ロード バランシングの直接の結果である可能性があります。

解決方法

アップストリーム スイッチが 4.1(3) 以上のコードを実行している MDS スイッチであり、なおかつ NPV F_Port トランキングに対応したスイッチである場合、推奨されるコンフィギュレーションは F_Port トランキング ポート チャネリング機能を実行することです。

例（NPIV コア）：

```
pod3-9222i(config)# feature npiv
pod3-9222i(config)# feature fport-channel-trunk

pod3-9222i(config)# interface port-channel 1
pod3-9222i(config-if)# switchport mode f
pod3-9222i(config-if)# switchport trunk mode on
pod3-9222i(config-if)# channel mode active
pod3-9222i(config-if)# interface fc2/13, fc2/19
pod3-9222i(config-if)# switchport mode f
pod3-9222i(config-if)# switchport rate-mode dedicated
pod3-9222i(config-if)# switchport trunk mode on
pod3-9222i(config-if)# channel-group 1 force
```

この例では、fc2/13 と fc2/19 がポートチャネル 100 に追加され、ディセーブルになります。ポートチャネルの相手側のスイッチでも同じ操作を行い、両方で「no shutdown」を実行して両インターフェイスを起動します。

例：

```
pod3-9222i(config-if)# no shut
```

例（NPV エッジ）：

```
pod7-5020-51(config)# interface san-port-channel 1
pod7-5020-51(config-if)# switchport mode np
pod7-5020-51(config-if)# switchport trunk mode on
pod7-5020-51(config-if)# interface fc2/1-2
pod7-5020-51(config-if)# switchport mode np
pod7-5020-51(config-if)# switchport trunk mode on
pod7-5020-51(config-if)# channel-group 1
```

この例では、fc2/1 と fc2/2 がポートチャネル 1 に追加され、ディセーブルになります。ポートチャネルの相手側のスイッチでも同じ操作を行い、両方で「no shutdown」を実行して両インターフェイスを起動します。

例：

```
pod7-5020-51(config-if)# no shut
```

ダウンストリーム NPV エッジ スイッチ上のサーバがファブリックにログインしない

ダウンストリーム NPV エッジ スイッチに接続されたサーバがファブリックにログインしません。

考えられる原因

ダウンストリーム NPV エッジ スイッチ上のサーバがファブリックにログインしないか、「waiting for FLOGI」メッセージが表示されます（両方が起こる場合もあります）。

例：

```
switch# show npv status
npiv is enabled
Server Interfaces:
==================
Interface: fc1/6, VSAN: 1, NPIV: No, State: Waiting for FLOGI
```

解決方法

- NPV エッジ スイッチとコア スイッチの両方の設定を確認します。F_Port トランキング機能を実行していない場合は、VSAN の不一致がないこと、およびサーバ ポート、NPV NP ポート、NPIV コア F_Port、ストレージ ポートがすべて同じ VSAN に属していてオンラインになっていることを確認します。
- 設定が正しい場合は、問題の所在を突き止めるために Ethanalyzer トレースを収集して、Fabric Login（FLOGI）フレームが受信されていること、Fabric Discovery（FDISC）コマンドとして NPIV コアに送信されていることを確認できます。

  Ethanalyzer トレースの例：

  ```
  switch# ethanalyzer local sniff-interface inbound-hi display-filter "!llc && !stp"
  limit-captured-frames 0 write bootflash:npv-trace
  Capturing on eth4
  ```

- NPV に接続されたサーバ ポートをフラップすることにより、問題を再現します。トレースがブートフラッシュに書き込まれるので、その内容を次のコマンドを使用してスイッチから別の場所にコピーします。

  ```
  copy bootflash: ftp:
  ```

- トレースをコピーしたら、Wireshark を使用してトレースを開き、フローを検証します。

  通常の NPV ログイン フローの例：

```
Server --------------------> FLOGI ----------> NPV Edge Switch  Fabric Login frame =
                                                                FLOGI

NPV Edge Switch ------> FDISC ----------> NPIV Core Switch      Fabric DISCovery
                                                                frame maps parameters
                                                                from Server FLOGI
```

```
NPV Core Switch ------> Accept ---------> NPV Edge Switch       NPIV Core assigns an
                                                                FCID with the Accept
                                                                to the FDISC from NPV
                                                                Edge Switch

NPV Edge Switch ------> Accept ---------> Server                Accept to original
                                                                Server FLOGI with FCID
                                                                assigned from NPIV
                                                                Core Switch
```

サーバが物理的に接続されている正確なポートの特定

NPIV スイッチからは、ダウンストリーム NPV 接続サーバが接続されている物理ポートはわかりません。次の手順を使用して、その物理ポートを特定できます。

考えられる原因

NPIV コア スイッチに複数のダウンストリーム NPV エッジ スイッチが接続されている場合、サーバが物理的に接続されている正確なポートを特定するには、次の手順を実行します。

解決方法

- サーバの PWWN と、それに対応するサーバの接続先スイッチを特定します。

  例：

  ```
  NPIV-Core(config-if)# show flogi database

  fc1/16 100 0xee00e4 21:00:00:04:cf:17:66:b7 20:00:00:04:cf:17:66:b7
  fc1/16 100 0xee00e8 21:00:00:04:cf:17:66:0e 20:00:00:04:cf:17:66:0e
  fc1/25 100 0xee0100 20:41:00:0d:ec:a3:da:40 20:64:00:0d:ec:a3:da:41
  fc1/26 100 0xee0200 20:42:00:0d:ec:a3:da:40 20:64:00:0d:ec:a3:da:41
  fc1/26 100 0xee0201 21:00:00:c0:dd:12:04:f3 20:00:00:c0:dd:12:04:f3
  ```

  この例では、サーバは次の行によって特定されます。

  ```
  fc1/26 100 0xee0201 21:00:00:c0:dd:12:04:f3 20:00:00:c0:dd:12:04:f3
  ```

  スイッチは次の行によって特定されます。

  ```
  fc1/26 100 0xee0200 20:42:00:0d:ec:a3:da:40 20:64:00:0d:ec:a3:da:41
  ```

- NPV エッジ スイッチの IP アドレスを特定します。

  例：

  ```
  NPIV-Core(config-if)# sh fcns database npv
  VSAN 100:

  20:64:00:0d:ec:a3:da:41 172.18.217.51 fc2/1 20:00:00:0d:ec:51:0c:00 fc1/25
  20:64:00:0d:ec:a3:da:41 172.18.217.51 fc2/2 20:00:00:0d:ec:51:0c:00 fc1/26
  ```

- NPV エッジ スイッチに telnet します。

  例：

  ```
  NPIV-Core(config-if)# telnet 172.18.217.51
  ```

- サーバの PWWN を特定します。

  例：

```
switch-NPV-Edge# show npv flogi-table

vfc3 100 0xee0201 21:00:00:c0:dd:12:04:f3 20:00:00:c0:dd:12:04:f3 fc2/2
```

- 上の例に示すようにインターフェイスが FCoE（VFC）インターフェイスである場合は、show interface vfc3 コマンドを使用して、VFC の物理的な宛先ポートを確認します。

4.2(1)N1 F_Port トランキング機能を設定した後、VSAN が初期化ステートでスタックしている

F_Port トランキング ポート チャネル、またはポート チャネルのトランキング メンバーに対して show interface コマンドを実行すると、特定の VSAN が初期化ステートにあり、オンラインになっていません。

考えられる原因

4.2(1)N1 F_Port トランキング機能を設定した後、トランク ポート上の VSAN が初期化ステートでスタックしているように見えます。

例：

```
switch(config-if)# sh int fc2/1
fc2/1 is trunking
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:41:00:0d:ec:a4:3b:80
Admin port mode is NP, trunk mode is on
snmp link state traps are enabled
Port mode is TNP
Port vsan is 1
Speed is 4 Gbps
Transmit B2B Credit is 16
Receive B2B Credit is 16
Receive data field Size is 2112
Beacon is turned off
Belongs to san-port-channel 200
Trunk vsans (admin allowed and active) (1,99,200)
Trunk vsans (up) (1,99)
Trunk vsans (isolated) ()
Trunk vsans (initializing) (200)
```

Fabric Manager の [Trunk Failures] タブでも、トランク VSAN がリスト表示される場合があります。ただし、これは通常の状態である可能性があります。ある特定の VSAN にダウンストリーム デバイスが 1 つもログインしていない場合、その VSAN は初期化ステートにとどまります。

解決方法

次のコマンドを使用して、問題の VSAN にログインしているデバイスがあるかどうかを確認します。

例：

```
switch# show npv flogi-table

fc2/7 99 0xba0002 10:00:00:00:00:02:00:00 10:00:00:00:00:00:02:00 Spo200
fc2/8 99 0xba0003 10:00:00:00:00:01:00:00 10:00:00:00:00:00:01:00 Spo200
Total number of flogi = 2.
```

上の例では、VSAN 200 にログインしているデバイスはありません。

ゾーン分割

ゾーンセットをアクティブにできず、拡張ゾーン分割モードでゾーン分割を設定できない

ゾーンセットをアクティブにできず、拡張ゾーン分割モードでゾーン分割を設定できません。エラーメッセージ「Zoning database update in progress, command rejected」を受け取る場合があります。

考えられる原因

同じスイッチ上または別のスイッチ上の別のユーザが拡張ゾーン分割設定のロックを保持しています。

解決方法

一般的な方法は、ゾーン分割ロックを解放することです。

ステップ 1　ロックを保持しているスイッチ（ドメイン/IP アドレス）を特定します。

ステップ 2　そのスイッチ上のロックを保持しているユーザを特定します。

ステップ 3　そのスイッチ上のそのユーザのロックをクリアします。

- 同じスイッチで「show zone status vsan <vsan-id>」コマンドを実行して、ロックを保持しているユーザを特定します。

  例：

  ```
  switch1# show zone status vsan 200
  VSAN: 200 default-zone: deny distribute: active only Interop: default
  mode: enhanced merge-control: allow
  session: remote [dom: 121][ip: 171.165.98.20] <<==
  ```

  この例では、IP アドレスが 171.165.98.20 のリモート スイッチがロックを保持しています。
- リモート スイッチに接続し、コマンド「show zone status vsan」を実行します。

  例：

  ```
  switch2# show zone status vsan 200

  VSAN: 200 default-zone: deny distribute: active only Interop: default
  mode: enhanced merge-control: allow
  session: cli [remi] <<==
  ```

  この例では、ユーザ「Remi」が拡張ゾーン分割のロックを保持しています。
- リモート スイッチ（上の例では N5K2）で、コマンド「no zone commit vsan <vsan-id>」を使用してロックを解放します。
- ロックがクリアされたことを確認するには、コマンド「show zone status vsan <vsan-id>」を実行します。

  この時点で、session パラメータは「none」と表示されます。
- ロックがまだ残っている場合は、コマンド「clear zone lock」を使用して、ロックを保持しているスイッチからロックを解除します。
- それでもロックが残っている場合は、次のコマンドを使用して、詳細な分析に役立つ情報を収集します。

```
show zone internal vsan <vsan-id>
show zone status vsan <vsan-id>
show fcdomain domain-list vsan <vsan-id>
show users
show tech-support zone
show tech-support device-alias
show logging
```

ホストがストレージと通信できない

SAN の初期導入時または SAN のトポロジ変更後に、一部のホストがストレージと通信できない場合があります。イニシエータが、ストレージ アレイ内のそれらのホスト用に割り当てられた LUN にアクセスできません。

考えられる原因

ホストとストレージが 2 つの異なるスイッチに接続している場合は、ISL リンク、つまり両方のスイッチに接続している xE ポートが分離されている可能性があります。

特定の VSAN 内で xE ポートが分離される原因としては、次が考えられます。

- ファブリック タイマーの設定ミス
- ポート パラメータの設定ミス
- ゾーン分割の不一致

解決方法

TE ポートでの VSAN 分離を解決する方法は次のとおりです。

- TE ポートで「show interface fc slot/port」コマンドを使用して、VSAN 番号を確認します。

  分離された VSAN の番号は、ホストおよびストレージが接続している VSAN の番号と一致している必要があります。

  コマンド出力で、「Trunk vsans (isolated) (Vsan <vsan-id>)」を確認します。
- 「show port internal info interface fc slot/port」コマンドを使用して、VSAN 分離の根本原因を突き止めます。

考えられる原因

ホストとストレージが同じ VSAN に属していません。

解決方法

- 「show vsan membership」コマンドを使用して、ホストとストレージの両方が同じ VSAN に属しているかどうかを確認します。
- ホストとストレージが異なる VSAN に属している場合は、コンフィギュレーション モードでコマンド「vsan database」と「vsan vsan-id interface fc slot/port」を使用して、ホストおよびストレージ デバイスに接続されたインターフェイスを同じ VSAN に移動します。

考えられる原因

ホストとストレージが同じゾーンに属していません。ゾーンがアクティブ ゾーンセットに含まれていません。アクティブ ゾーンセットが存在せず、デフォルトのゾーン ポリシーが拒否に設定されています。

解決方法

- コマンド「show zone status vsan-id」を使用して、デフォルトのゾーン ポリシーが拒否に設定されているかどうかを確認します。

例：

```
switch# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
```

ステート「default zone policy permit」は、どのノードからも他のすべてのノードが見えることを意味します。deny は、明示的にゾーンに配置されていないノードはすべて分離されることを意味します。

ゾーン分割を使用していない場合は、「zone default-zone permit」を使用してデフォルトのゾーン ポリシーを変更できますが、これはベスト プラクティスではありません。

- ホストとストレージに対してコマンド「show zone member」を使用して、両者が同じゾーンに属しているかどうかを確認します。同じゾーンに属していない場合は、コマンド「zone name zonename vsan-id」を使用して、その VSAN 内にゾーンを作成します。

  例：

  ```
  switch(config)# zone name testzone vsan 100
  switch(config-zone)# member pwwn 21:00:00:20:37:9e:02:3e
  switch(config-zone)# member pwwn 21:00:00:c0:dd:12:04:ce
  ```

  コマンド「show zone vsan vsan-id」を使用して、ホストとストレージが同じゾーンに配置されたことを確認します。

- コマンド「show zoneset active vsan vsan-id」を使用して、アクティブ ゾーンセットの名前を確認します。

  ホストとストレージを含むゾーンがアクティブ ゾーンセットに含まれていない場合は、コンフィギュレーション モードでコマンド「zoneset name」を使用してゾーンセット サブ モードに入り、「member」コマンドを使用してゾーンをアクティブ ゾーンセットに追加します。

  例：

  ```
  switch(config)#zoneset name testzoneset vsan 100
  switch(config-zoneset)#member testzone
  ```

- 「zoneset activate」コマンドを使用して、ゾーンセットをアクティブにします。

  例：

  ```
  switch(config)# zoneset activate testzoneset vsan 100
  ```

2 つのスイッチが E または TE ポートを使用して接続しているときにゾーン結合が失敗する

2 つのスイッチが E または TE ポートを使用して接続しているとき、ゾーン結合が失敗する場合があります。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone merge failure, isolating interface fc2/1 error:
Received rjt from adjacent switch:[reason:0]
%ZONE-2-ZS_MERGE_FAILED: %$VSAN 1%$ Zone merge failure, isolating interface fc1/2 error:
Member mismatch
%ZONE-2-ZS_MERGE_ADJ_NO_RESPONSE: Adjacent switch not responding,isolating interface
%ZONE-2-ZS_MERGE_FULL_DATABASE_MISMATCH: Zone merge full database mismatch on interface
```

考えられる原因

2 つのスイッチが同じゾーンセット名とゾーン名を持っているにもかかわらず、それらのゾーン メンバーが異なっている可能性があります。

スイッチ ファブリックを結合するときは、両方のアクティブ ゾーン セットに含まれるゾーンの名前が重複していないか、同じ名前を持つゾーンが正確に同じメンバーを持つ必要があります。これらの条件がどちらも満たされない場合、2 つのファブリックを接続する E ポートは分離した状態になります。

スイッチ ファブリックを結合するプロセスは次のとおりです。

- ソフトウェアがプロトコル バージョンを比較します。プロトコル バージョンが異なる場合、ISL は分離されます。
- プロトコル バージョンが同じである場合、ゾーン ポリシーが比較されます。ゾーン ポリシーが異なる場合、ISL は分離されます。
- ゾーン結合オプションが同じである場合、結合制御設定に基づいて比較が行われます。
  - 設定が「制限」の場合、アクティブ ゾーン セットとフル ゾーン セットが同じである必要があります。これらが同じでない場合、リンクは分離されます。
  - 設定が「許可」の場合、結合ルールを使用して結合が行われます。ホストとストレージが同じゾーンに属していません。ゾーンがアクティブ ゾーンセットに含まれていません。アクティブ ゾーンセットが存在せず、デフォルトのゾーン ポリシーが「拒否」に設定されています。

解決方法

ゾーン結合が失敗した場合、この問題は次のいずれかの方法を使用して解決できます。

- 両方のゾーンセットのゾーン メンバーが一致するよう修正し、競合を解消します。
  - 両方のスイッチで「show zoneset active vsan vsan-id」コマンドを使用して、ゾーンと各ゾーンのメンバーを比較します。
  - いずれかのゾーンのメンバーシップを変更して、同じ名前を持つ他のゾーンに合わせます。
- いずれかのスイッチでゾーンセットを非アクティブにし、ゾーン結合プロセスをもう一度行います。
  - 「no zoneset activate name zonesetname vsan-id」コマンドを使用して、いずれかのスイッチのゾーンセット設定を非アクティブにします。
  - 「show zoneset active」コマンドを使用して、ゾーンセットが削除されたことを確認します。
  - 「shutdown」コマンドを使用して結合するゾーンへの接続をシャットダウンしてから、「no shutdown」コマンドを使用して結合するゾーンへの接続を再びアクティブにします。
  - 「show zoneset active vsan-id」を使用してすべてのメンバーが正しいことを確認し、「show interface fc slot/port」を使用して VSAN が分離されていないことを確認します。
- スイッチ間でゾーンセットを明示的にインポートまたはエクスポートして、両スイッチを同期します。
  - 「zoneset import interface interface-number vsan vsan-id」コマンドまたは「zoneset export interface interface-number vsan vsan-id」コマンドを使用して、いずれかのスイッチでアクティブ ゾーンセットを上書きします。
  - 「show interface fc slot/port」を使用して、この中断操作の後に VSAN が分離されていないことを確認します。

ゾーンセットのアクティブ化の失敗

ゾーンセットのアクティブ化が失敗したとき、「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
ZONE-2-ZS_CHANGE_ACTIVATION_FAILED: Activation failed.
ZONE-2-ZS_CHANGE_ACTIVATION_FAILED_RESN: Activation failed : reason
```

考えられる原因

ゾーン データベースのサイズが 2048 KB を超えているときに新しいスイッチがファブリックに加入した場合、ゾーンセットのアクティブ化が失敗することがあります。

解決方法

- 「show zone analysis active vsan vsan-id」コマンドを使用して、アクティブ ゾーンセット データベースを分析します。フォーマット サイズが 2048 KB を超えていないかどうかを確認します。

  2048 KB の上限を超えている場合は、ゾーンまたはゾーン内のデバイスをいくつか削除する必要があります。

  例：

  ```
  switch# show zone analysis active vsan 100
  Zoning database analysis vsan 100
  Active zoneset: vsm_vem_v100_zs [-]
  Activated at: 13:13:44 UTC May 27 2010
  Activated by: Merge [ Interface san-port-channel 100 ]
  Default zone policy: Deny
  Number of devices zoned in vsan: 1/9 (Unzoned: 8)
  Number of zone members resolved: 1/3 (Unresolved: 2)
  Num zones: 1
  Number of IVR zones: 0
  Number of IPS zones: 0
  Formatted size: 92 bytes / 2048 Kb
  ```

- 「show zone internal change event-history vsan vsan-id」コマンドを使用して、ゾーンセット アクティブ化の問題があるかどうかを確認します。
- この問題をさらにトラブルシューティングするには、「show tech-support zone」コマンドと「show logging log」コマンドの出力をキャプチャします。

2 つのスイッチ間でのフル ゾーン データベース同期の失敗

2 つのスイッチが E または TE ポートを使用して接続していて、それらのスイッチが異なるゾーンセット配信ポリシーを持つとき、フル ゾーン データベース同期が失敗する場合があります。ファブリックの分離/結合の結果として、あるファブリックの実行コンフィギュレーションにフル ゾーンセット データベースが含まれないことがあります。

考えられる原因

ゾーンセットの配信は、隣接スイッチへの結合要求の送信時、またはゾーンセットのアクティブ化の際に行われます。

ゾーン配信ポリシーは 2 つのスイッチで異なるように設定できますが、そうすると同期が失敗する場合があります。

解決方法

「show zone status」コマンドを使用して、両方のスイッチの配信ポリシーを確認します。

例：

```
VSAN: 100 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
```

配信ポリシーが「active only」に設定されている場合は、アクティブ ゾーンセットが配信されます。また、配信ポリシーがフルに設定されていることも確認します。

コンフィギュレーション モードで VSAN ごとにすべてのスイッチへのフル ゾーン セットおよびアクティブ ゾーン セットの配信をイネーブルにするには、「zoneset distribute full vsan vsan-id」コマンドを使用します。

VSAN 内のスイッチのデフォルト ゾーン ポリシーの不一致が原因で、ストレージへのアクセス時に予期しない結果が起こる

基本ゾーン モードで VSAN 内のすべてのスイッチのデフォルト ゾーン ポリシーが一致していない場合、ホストがストレージにアクセスするときに予期しない結果が起こる場合があります。

考えられる原因

デフォルト ゾーン ポリシーが「permit」に設定されていて、VSAN にアクティブ ゾーンセットがない場合は、その VSAN のどのメンバーからも他のすべてのノードが見えます。

解決方法

1 つの方法は、ゾーン運用モードを基本から拡張に移行することです。拡張ゾーン分割では、ゾーン設定が VSAN 内のすべてのスイッチ間で同期されます。これにより、デフォルト ゾーン ポリシーが一致しない可能性はなくなります。

- 「show zone status」コマンドを使用して、ゾーンのステータスを表示します。

  ```
  VSAN: 300 default-zone: deny distribute: active only Interop: default
  mode: basic merge-control: allow
  ```

- 「zone default-zone」コマンドを使用してデフォルト ゾーン ポリシーを設定し、「zone mode enhanced vsan-id」コマンドを使用して運用モードを拡張ゾーン分割モードに設定します。

解決方法

もう 1 つの方法を次に示します。

- VSAN 内のすべてのスイッチで「show zone status」を使用して、運用モードとデフォルトゾーン ポリシーを確認します。
- 「zone mode basic」コマンドを使用して、基本モードでないスイッチをすべて変更します。
- VSAN 内の各スイッチで「zone default-zone」コマンドを使用して、同じデフォルト ゾーン ポリシーを設定します。

SAN PortChannel

スイッチを SAN PortChannel 経由で接続しようとするとファイバ チャネル ポートがダウンする

スイッチを SAN PortChannel 経由で接続しようとすると、ファイバ チャネル ポートがダウンします。

「show interface brief」コマンドを実行すると、次のように出力されます。

```
fc slot/port is down (Error disabled - Possible port channel misconfiguration)
```

考えられる原因

コンフィギュレーションでいずれかの SAN ポートチャネル互換性パラメータの設定が間違っています。

互換性チェックでは、チャネルのすべての物理ポートで同一のパラメータ設定が確実に使用されるようにします。そうでない場合、ポートが PortChannel に所属できません。互換性チェックは、ポートを PortChannel に追加する前に実施します。

互換性チェックでは、PortChannel の両側で次のパラメータと設定が一致していることを確認します。

- 機能パラメータ
  (インターフェイスのタイプ、両側ともギガビット イーサネットまたは両側ともファイバ チャネル)。
- 管理互換性パラメータ
  (速度、モード、レート モード、ポート VSAN、許可 VSAN リスト、ポート セキュリティ)。
- 動作パラメータ
  (リモート スイッチ WWN とトランキング モード)。

解決方法

- 「show san-port-channel compatibility-parameters」を使用して、コンフィギュレーションでチェックするパラメータを確認します。

  一般に、コンフィギュレーションを修正して FC ポートを shut/no shut した場合、ポートは正常に回復します。
- 別のエラー メッセージが表示されて問題が解決しない場合は、次のいずれか、または複数のコマンドを実行してさらにデバッグします。

```
show port internal info interface fc slot/port
show port internal event-history interface fc slot/port
show san-port-channel internal event-history errors
show logging log | grep fc slot/port
show san-port-channel internal event-history all
show tech-support detail > bootflash:showtechdet
```

新しく追加したファイバチャネル インターフェイスが SAN PortChannel でオンラインにならない

新しいファイバチャネル インターフェイスを追加したとき、そのインターフェイスが SAN PortChannel でオンラインになりません。

設定操作時に次のエラー メッセージが表示される場合があります。

「Command failed: port not compatible [reason]」

考えられる原因

ポート チャネル モードが「on」に設定されています。

スイッチ間の不整合な状態を防ぐため、およびスイッチ間の整合性を維持するためにデフォルトの ON モードを使用した場合、ポートはシャットダウンします。

解決方法

「no shutdown」を使用して、ポートを再び明示的にイネーブルにします。

考えられる原因

インターフェイス パラメータが既存の SAN PortChannel と互換性がありません。

解決方法

force オプションを使用して、物理インターフェイスに SAN PortChannel のパラメータを受け入れるよう強制します。インターフェイス サブ コンフィギュレーション モードで、「channel-group <channel-group number> force」コマンドを使用します。

トランキングを設定できない

インターフェイス コンフィギュレーション モードでトランキングを設定できません。

CLI 出力に次のエラー メッセージが表示される場合があります。

「error:invalid switchport config」

考えられる原因

トランキング プロトコルがディセーブルになっています。

解決方法

「trunk protocol enable CLI」コマンドを使用して、トランキングをイネーブルにします。

VSAN トラフィックがトランクを通過しない

VSAN トラフィックがトランクを通過できません。

ホストから、同じ VSAN に属していて、なおかつ TE ポートを使用して 2 つの異なるスイッチに接続されたターゲットにアクセスできません。VSAN トラフィックがトランクを通過できません。ホストからターゲットへのパスによっては、パフォーマンスが低下する場合や、どのディスクにもアクセスできない場合があります。

考えられる原因

VSAN が allowed-active VSAN リストに登録されていません。

解決方法

「switchport trunk allowed vsan CLI」コマンドを使用して、VSAN を allowed-active リストに追加します。

SAN PortChannel のインターフェイスの下にある特定の VSAN で xE ポートが分離される

SAN PortChannel のインターフェイスの下にある特定の VSAN で xE ポートが分離されます。

ロギング ログに次のエラー メッセージが表示される場合があります。

「%$VSAN <VSAN#>%$ Interface port-channel <channel #>, vsan <vsan #> is down (isolation due to [cause])」

考えられる原因

特定の VSAN 内で xE ポートが分離される原因としては、次が考えられます。

- ファブリック タイマーの設定ミス
- ポート パラメータの設定ミス
- ゾーン分割の不一致

解決方法

TE ポートでの VSAN 分離を解決するには、TE ポートで「show interface fc slot/port」コマンドを使用して VSAN 番号を確認します。分離された VSAN の番号は、ホストおよびストレージが接続している VSAN の番号と一致している必要があります。

コマンドの出力で、「Trunk vsans (isolated) (Vsan <number>)」のような情報を探します。

「show port internal info interface san-port-channel <number>」コマンドを使用して、VSAN 分離の原因を突き止めます。

SAN ポートチャネル インターフェイスが作成できない

SAN ポートチャネル インターフェイスが作成できません。

コンフィギュレーション モード時に次のエラー メッセージが表示される場合があります。

「failed to create port-channel channel-id:」

考えられる原因

ユーザは次のメッセージを受け取ります。

failed to create port-channel channel-id: all port-channels have been created [max channel number reached]

（注）　SAN ポートチャネルは最大 4 つ作成できます（NX-OS 4.2(1)N1(1) を含む）。これはソフトウェアの制限です。

解決方法

特定の番号を持つ SAN ポートチャネルを作成する場合に、4 つの SAN ポートチャネルがすでに設定されているときは、使用頻度の低いいずれかの SAN ポートチャネルを削除する必要があります。「no interface san-port-channel x」コマンドを使用して、いずれかの SAN ポートチャネルを削除します。

考えられる原因

ユーザは次のメッセージを受け取ります。

Channel group X is already an Ethernet port channel

解決方法

SAN ポートチャネルを設定する際に 1 ～ 256 の範囲の別の番号を選択する必要があります。

「show port-channel usage」コマンドを使用して、既存のポートチャネルで使用されている番号を確認します。

例：

```
show port-channel usage
Total 3 port-channel numbers used
============================================
Used : 198 - 199 , 500
Unused: 1 - 197 , 200 - 499 , 501 - 4096
(some numbers may be in use by SAN port channels)
```

FC サービス

ここでは、シスコ ファイバ チャネル サービスのトラブルシューティングの概要を示し、一般的な問題とその解決方法について説明します。

概要

ファイバ チャネル ファブリックは、そのクライアント（ファイバ チャネル ノード）に対して一連のサービスを提供します。各ノードはこれらのファイバ チャネル サービス（FC サービス）を使用してストレージ ネットワークとやり取りし、接続ステート、接続パラメータ、設定、トポロジ変更などの情報を交換します。

FC サービスには、Well Known Address（WKA; well-known アドレス）を持つポートへのログインを通じてアクセスできます。WKA は、ファブリックの内部使用（通常はファブリック サービス）のために予約されているポート FC ID です。

次の表に、well-known アドレスと各アドレスに関連するサービスを示します。
（出典：www.t11.org）

well-known アドレス	説明
x'FF FC 01' ～ x'FF FC FE'	ドメイン コントローラのために予約済み
x'FF FF F0'	N_Port コントローラのために予約済み
x'FF FF F1' ～ x'FF FF F3'	予備
x'FF FF F4'	イベント サービス（FC-GS-5）
x'FF FF F5'	マルチキャスト サーバ（FC-PH3）
x'FF FF F6'	クロック同期サーバ（FC-PH3）
x'FF FF F7'	セキュリティ キー配信サービス（FC-PH3）
x'FF FF F8'	エイリアス サーバ（FC-PH2）
x'FF FF F9'	Quality of Service Facilitator-Class4（FC-PH2）
x'FF FF FA'	管理サービス（FC-GS-5）
x'FF FF FB'	タイム サービス（FC-GS-5）

well-known アドレス	説明
x'FF FF FC'	ディレクトリ サービス（FC-GS-5）
x'FF FF FD'	ファブリック コントローラ
x'FF FF FE'	F_Port コントローラ
x'FF FF FF'	ブロードキャスト アドレス/サーバ

ファイバ チャネル ポートが初期化ステートにとどまる

ファイバ チャネル F タイプ ポートがオンラインにならず、初期化ステートでスタックしています。

「show interface fc slot/port」コマンドを実行すると、次のように出力されます。

```
fc slot/port is down (Initializing)
```

ファイバ チャネル ポートは、リンク レベル初期化が正常に完了した後、初期化ステートに入ります。F タイプ ポートでは、次のステップは FLOGI（ファブリック ログイン）プロセスを完了することです。ポートは FLOGI プロセスが完了するまで初期化ステートにとどまります。

考えられる原因

リンク パートナーがバイパス モードになったことが原因で、ポートがアップしています。

解決方法

「show hardware internal fc-mac <slot-number> port <port-number> statistics」コマンドを使用して、リンク初期化が正常に完了した後に Class-3 入力カウンタが増加しているかどうかを確認します。

例：

```
switch# show hardware internal fc-mac 2 port 1 statistics
 ADDRESS     STAT                                                  COUNT
__________ ________                                          ____________________
0x0000003c FCP_CNTR_MAC_RX_LOSS_OF_SYNC                                     0x1
0x0000003d FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER                          0x50
0x00000042 FCP_CNTR_MAC_CREDIT_IG_XG_MUX_SEND_RRDY_REQ                    0x152
0x00000043 FCP_CNTR_MAC_CREDIT_EG_DEC_RRDY                                 0x7c
0x00000061 FCP_CNTR_MAC_DATA_RX_CLASS3_FRAMES                             0x130
0x00000062 FCP_CNTR_MAC_DATA_RX_CLASSF_FRAMES                              0x22
0x00000069 FCP_CNTR_MAC_DATA_RX_CLASS3_WORDS                           0x61c98
0x0000006a FCP_CNTR_MAC_DATA_RX_CLASSF_WORDS                             0xff0
0x00000065 FCP_CNTR_MAC_DATA_TX_CLASS3_FRAMES                              0x52
0x00000066 FCP_CNTR_MAC_DATA_TX_CLASSF_FRAMES                              0x2a
0x0000006d FCP_CNTR_MAC_DATA_TX_CLASS3_WORDS                            0x944c
0x0000006e FCP_CNTR_MAC_DATA_TX_CLASSF_WORDS                             0xec4
0xffffffff FCP_CNTR_LINK_RESET_IN                                           0x1
0xffffffff FCP_CNTR_OLS_IN                                                  0x1
0xffffffff FCP_CNTR_NOS_IN                                                  0x1
0xffffffff FCP_CNTR_LRR_IN                                                  0x2
0xffffffff FCP_CNTR_LINK_RESET_OUT                                          0x1
0xffffffff FCP_CNTR_OLS_OUT                                                 0xa
0xffffffff FCP_CNTR_NOS_OUT                                                 0x2
0xffffffff FCP_CNTR_LRR_OUT                                                 0xb
0xffffffff FCP_CNTR_LINK_FAILURE                                            0x2
```

考えられる原因

FLOGI パケットが、FC-MAC から FLOGI サーバまでのデータ パス上のどこかでドロップされました。

解決方法

次の方法を検討します。

- 「show hardware internal fc-mac <slot-number> port <port-number> statistics」コマンドを使用して、Class-3 パケットのカウンタを確認します。
- 「show flogi internal all interface fc slot/port」コマンドの出力を分析し、パス上のどこで FLOGI パケットのドロップが起こり得るかを調べます。
- 「Fport server fault-injection」テーブルをチェックし、「Invalid」、「Drop」の FLOGI パケットがないかどうかを確認します。
- 「shut」CLI コマンド、「no shut」コマンドの順に入力して、FC スロット/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 FC モジュールの別のポートまたは他の FC モジュールのポートに接続を移動してみます。
- それでも問題が解決しない場合は、次のコマンドを使用して、詳細な分析に役立つ情報を収集します。

```
Show tech-support flogi
Show logging log | grep  fc slot/port
show port internal info interface fc slot/port
show port internal event-history interface fc slot/port
show tech-support detail > bootflash:showtechdet
show platform fwm info pif fc slot/port {find the gatos instance for the port}
show platform fwm info gatos-errors 13 {check for the non-zero counters for drops}
```

次のコマンドを使用して、debug flogi をキャプチャします。

```
switch# debug logfile flogi_debug
switch# debug flogi all
switch(config)# int fc slot/port
switch(config-if)# shut
switch(config-if)# no shut
switch(config-if)# undebug all
switch# dir log:  {check if you have the file in log: directory}
         31     Aug 03 13:45:13 2010  dmesg
      34941     Aug 06 07:21:15 2010  flogi_debug

switch# copy log:flogi_debug ftp://x.y.z.w {or use tftp/scp/sftp}
```

特定の VSAN トラフィックが SAN ファブリック経由でルーティングされない

VSAN の実装では、設定された各 VSAN がそれぞれ異なるファブリック サービスのセットをサポートできます。そのようなサービスの 1 つに FSPF ルーティング プロトコルがあります。このプロトコルは VSAN ごとに個別に設定できます。不適切なトラフィック エンジニアリング機能が使用されている場合、特定の VSAN トラフィックがルーティングされないことがあります。

考えられる原因

FSPF hello 間隔が適切に設定されていません。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
FSPF-3-HELLO_MISMATCH: %$VSAN <vsan-id>%$ Mismatch in Hello timer in the Hello packet on
interface san-port-channel <channel-id>
%FSPF-3-FC2_PROC_ERR: %$VSAN <vsan-id>%$ Error in processing HELLO  packet on interface
san-port-channel <channel-id>, Error  = Bad packet received
```

解決方法

NX-OS CLI を使用して ISL 上の不適切な hello 間隔を解決するには、次の手順を実行します。

ステップ 1　「debug fspf all」コマンドを使用して不適切な hello 間隔のメッセージを探すか、「show logging」ログの最後のメッセージをチェックしてエラー メッセージを探します。

デバッグ出力では、次のメッセージが生成されます。

```
fspf: Wrong hello interval for packet on interface 40000c7 in VSAN 200
fspf: Error in processing hello packet , error = Bad packet received
```

ステップ 2　「undebug all」コマンドを使用して、デバッグをオフにします。

ヒント　ヒント：いずれかのデバッグ コマンドを入力する前に、telnet または SSH セッションをもう 1 つ開きます。デバッグ出力で現在のセッションがあふれた場合は、2 番目のセッションを使用して「undebug all」コマンドを入力し、デバッグ メッセージの出力を停止します。

ステップ 3　「show fspf vsan <vsan-id> interface」コマンドを使用して、両方のスイッチで FSPF の設定を表示します。

例：

```
switch# show fspf vsan 200 interface port-channel 200
FSPF interface port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 40 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT
Statistics counters :
   Number of packets received : LSU  3  LSA  3  Hello 136  Error packets 3
   Number of packets transmitted : LSU  3  LSA  3  Hello 182  Retransmitted LSU  0
   Number of times inactivity timer expired for the interface = 0


switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT

Statistics counters :
   Number of packets received : LSU  3  LSA  3  Hello 185  Error packets 169
   Number of packets transmitted : LSU  3  LSA  3  Hello 139  Retransmitted LSU  0
   Number of times inactivity timer expired for the interface = 24
```

（注）　この例では、

- 最初のスイッチでは、Hello タイマーがデフォルト（20 秒）に設定されていません。ネイバー スイッチ（Nexus 5000）の設定を確認して設定値を合わせます。
- FSPF が FULL ステートではありません。これは問題があることを示します。

ステップ 4　インターフェイス コンフィギュレーション モードで、両方のスイッチの fspf hello-interval が同じ値になるように変更します。

例：

```
switch(config)# interface san-port-channel 200
switch(config-if)# fspf hello-interval 40 vsan 200
```

ステップ 5　変更後、FSPF が FULL ステートになったことを確認します。

```
switch(config-if)# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 40 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x18(24)
Neighbor Interface is san-port-channel 200 (0x000400c7)

Statistics counters :
   Number of packets received : LSU  7  LSA  7  Hello 238  Error packets 218
   Number of packets transmitted : LSU  7  LSA  7  Hello 180  Retransmitted LSU  0
  Number of times inactivity timer expired for the interface = 32
```

考えられる原因

FSPF デッド間隔が適切に設定されていません。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%FSPF-3-HELLO_MISMATCH: %$VSAN <vsan-id>%$ Mismatch in Dead timer in the Hello packet on
interface san-port-channel <channel-id>
N5K-2 %FSPF-3-FC2_PROC_ERR: %$VSAN <vsan-id>%$ Error in processing HELLO  packet on
interface san-port-channel <channel-id>, Error  = Bad packet received
```

解決方法

NX-OS CLI を使用して ISL 上のデッド間隔の不一致を特定するには、次の手順を実行します。

ステップ 1　「debug fspf all」コマンドを使用して不適切なデッド間隔のメッセージを探すか、「show logging」ログの最後のメッセージをチェックしてエラー メッセージを探します。

デバッグ出力では、次のメッセージが生成されます。

```
fspf: Wrong hello interval for packet on interface 40000c7 in VSAN 200
fspf: Error in processing hello packet , error = Bad packet received
```

ステップ 2　「undebug all」コマンドを使用して、デバッグをオフにします。

ヒント　ヒント：いずれかのデバッグ コマンドを入力する前に、telnet または SSH セッションをもう 1 つ開きます。デバッグ出力で現在のセッションがあふれた場合は、2 番目のセッションを使用して「undebug all」コマンドを入力し、デバッグ メッセージの出力を停止します。

ステップ 3　「show fspf vsan <vsan-id> interface」コマンドを使用して、両方のスイッチで FSPF の設定を表示します。

例：

```
switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 120 s, Retransmit 5 s
FSPF State is INIT
```

```
Statistics counters :
   Number of packets received : LSU  4  LSA  4  Hello 27  Error packets 4
   Number of packets transmitted : LSU  4  LSA  4  Hello 38  Retransmitted LSU  0
   Number of times inactivity timer expired for the interface = 0

switch# show fspf vsan 200 interface port-channel 200
FSPF interface port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT

Statistics counters :
   Number of packets received : LSU  4  LSA  4  Hello 41  Error packets 35
   Number of packets transmitted : LSU  4  LSA  4  Hello 29  Retransmitted LSU  0
  Number of times inactivity timer expired for the interface = 4
```

（注） この例では、

- 最初のスイッチでは、デッド タイマーがデフォルト（80 秒）に設定されていません。ネイバー スイッチ（MDS）の設定を確認して設定値を合わせます。
- FSPF が FULL ステートではありません。これは問題があることを示します。

ステップ 4　インターフェイス コンフィギュレーション モードで、両方のスイッチの fspf dead-interval が同じ値になるように変更します。

```
switch(config)# interface san-port-channel 200
switch(config-if)# fspf dead-interval 80 vsan 200
```

ステップ 5　変更後、FSPF が FULL ステートになったことを確認します。「show fspf internal route vsan <vsan-id>」コマンドを使用して、VSAN トラフィックのルートがあることを確認します。

例：

```
switch# show fspf internal route vsan 200

FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost    Next hops
-----------------------------------------------
         200     0x18(24)          125 san-port-channel 200

switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x18(24)
Neighbor Interface is san-port-channel 200 (0x000400c7)

Statistics counters :
   Number of packets received : LSU  8  LSA  8  Hello 47  Error packets 4
   Number of packets transmitted : LSU  8  LSA  8  Hello 70  Retransmitted LSU  0
  Number of times inactivity timer expired for the interface = 0
```

考えられる原因

スイッチにリージョンの不一致があります。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%FSPF-3-BAD_FC2_PKT: %$VSAN 200%$ Received bad FC2 packet on interface san-port-channel
<channel-id>  : Packet received for non existant region in VSAN
```

解決方法

NX-OS CLI を使用してスイッチ上のリージョン不一致の問題を特定するには、次の手順を実行します。

ステップ 1　「show fspf vsan <vsan-id>」コマンドを使用して、VSAN に現在設定されているリージョンを表示します。

例（リージョン値は 2。デフォルトのリージョン値は 0）：

```
switch# show fspf vsan 200
FSPF routing for VSAN 200
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 2
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Local Domain is 0x22(34)
Number of LSRs = 1, Total Checksum = 0x00000c10

Protocol constants :
   LS_REFRESH_TIME = 30 minutes (1800 sec)
   MAX_AGE         = 60 minutes (3600 sec)

Statistics counters :
   Number of LSR that reached MaxAge = 0
   Number of SPF computations        = 0
   Number of Checksum Errors         = 0
   Number of Transmitted packets :  LSU 0 LSA 0 Hello 19 Retranmsitted LSU 0
   Number of received packets :  LSU 0 LSA 0 Hello 0 Error packets 18
```

ステップ 2　「debug fspf all」コマンドを使用して、存在しないリージョンに関するメッセージを探します。

例：

```
fspf: Hello timer reached for interface san-port-channel 200 in VSAN 200
fspf: FC2 packet received for non existant region 0 in VSAN 200
fspf: FC2 packet received for non existant region 0 in VSAN 200
```

ネイバー スイッチがアドバタイズしているリージョンは 0 です。FSPF は ISL ごとに INIT ステートにあります。

例：

```
switch# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT

Statistics counters :
   Number of packets received : LSU  0  LSA  0  Hello 0  Error packets 0
```

```
  Number of packets transmitted : LSU  0  LSA  0  Hello 49  Retransmitted LSU  0
 Number of times inactivity timer expired for the interface = 9
```

ステップ 3　「undebug all」コマンドを使用して、デバッグをオフにします。

ステップ 4　「show fspf vsan <vsan-id>」コマンドを使用して FSPF の設定を表示し、自律リージョンを確認します。

例：

```
switch# show fspf vsan 200
FSPF routing for VSAN 200
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 2
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Local Domain is 0x22(34)
Number of LSRs = 1, Total Checksum = 0x00000c10

switch# show fspf vsan 200
FSPF routing for VSAN 200
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 2000 msec
Local Domain is 0x18(24)
Number of LSRs = 2, Total Checksum = 0x00014f9f
```

ステップ 5　「fspf config vsan」コマンドを使用して FSPF コンフィギュレーション モードに入り、「region」コマンドを使用してリージョンを変更します。リージョンは、VSAN 内のすべてのスイッチで一致する必要があります。

例：

```
switch(config)# fspf config vsan 200
switch(config-(fspf-config))# region 0
```

無効な FLOGI が多すぎることが原因で、ファイバ チャネル ポートが一時停止する

NPV 機能がイネーブルになっている Cisco Nexus 5000、またはファブリック モードで動作している Cisco Nexus 5000 に接続されたファイバ チャネル ノードが、FLOGI 拒否が原因で SAN ファブリックにログインできません。

「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
%FLOGI-1-MSG_FLOGI_REJECT_FCID_ERROR: %$VSAN <vsan-id>%$ [VSAN <vsan-id>, Interface
fcslot/port/: mode[F]] FLOGI rejected - FCID allocation failed.
PORT-5-IF_DOWN_TOO_MANY_INVALID_FLOGIS: %$VSAN <vsan-id>%$ Interface fc slot/port is down
(Suspended due to too many invalid flogis
```

インターフェイスのステータスは「invalidFlogis」を示します。

```
show interface fc slot/port brief
fc slot/port      <vsan-id>      F      --      invalidFlogis
```

考えられる原因

その VSAN の FC ID 永続性テーブルがいっぱいになっている可能性があります。Nexus 5000 シリーズ スイッチが NPV エッジ スイッチとして設定されている場合は、NPV コア スイッチの FC ID 永続性テーブルがいっぱいになっている可能性があります。

FC ID：

Cisco Nexus 5000 シリーズ スイッチにログインした N ポートには、FC ID が割り当てられます。デフォルトでは、永続的 FC ID 機能はイネーブルです。この機能がディセーブルの場合は、次のようになります。

- N ポートが Cisco Nexus 5000 シリーズ スイッチにログインします。要求元 N ポートの WWN および割り当てられた FC ID が維持され、揮発性キャッシュに格納されます。揮発性キャッシュの内容は、再起動時に保存されません。
- スイッチは、FC ID と WWN のバインディングをベストエフォート方式で保持するように設計されています。たとえば、スイッチから 1 つの N ポートを切断したあとに、別のデバイスから FC ID が要求されると、この要求が許可されて、WWN と初期 FC ID の関連付けが解除されます。
- 揮発性キャッシュには、WWN と FC ID バインディング エントリを 4000 まで格納できます。このキャッシュが満杯になると、新しい（より最近の）エントリによって、キャッシュ内の最も古いエントリが上書きされます。この場合、最も古いエントリの対応する WWN と FC ID の関連付けが失われます。
- N ポートを取り外し、同じスイッチの任意のポートに接続すると、（このポートが同じ VSAN に属するかぎり）この N ポートには同じ FC ID が割り当てられます。

永続的 FC ID は、選択的に消去できます。現在使用中のスタティック エントリおよび FC ID は、削除できません。

解決方法

「show flogi internal」コマンドを使用して、FLOGI エラー メッセージを確認します。

例：

「show flogi internal event-history debugs」

```
222) Event:E_FLOGI_DEBUG, length:309, at 989582 usecs after Thu Jun 17
09:03:01 2010
fs_print_port_stats(10049): Port Stats for fc2/1, after cleanup:
   timestamp: Wed Jun 17 07:03:01 2010
   MSG_FLOGI: 52
   MSG_FC2_LS_RJT_OUT: 51
   EXCEPTION_CANNOT_ALLOCATE_FCID: 51
   EXCEPTION_TIMEOUT: 1
   EXCEPTION_FC2_INVALID_XCHG: 1
   tot_internal_exceptions: 51, since: Thu Dec 31 17:00:00 1969
```

「show flogi internal errors」

```
52) Event:E_DEBUG, length:119, at 977471 usecs after Thu Jun 17 09:03:01
2010
    [102] Interface fc2/1, nwwn 20:01:00:1b:32:af:d6:8c, pwwn
21:01:00:1b:32:af:d6:8c: flogi is valid; exchange is INVALID.
```

「show fcdomain address-allocation」コマンドを使用して FC ドメイン アドレス割り当てテーブルをチェックし、空き FC ID を確認します（NPV がイネーブルの場合は、NPV コア スイッチでこのコマンドを実行します）。

例：

「show fcdomain address-allocation」

```
VSAN 1
Free FCIDs: 0xe73f4f to 0xe73fff
            0xe7ff00 to 0xe7fffe

Assigned FCIDs: 0xe70000 to 0xe73f4e
                0xe74000 to 0xe7feff
                0xe7ffff

Reserved FCIDs: 0xe7ffff

Number free FCIDs: 432
Number assigned FCIDs: 65104
Number reserved FCIDs: 1
```

自動エリアリストおよび永続的 FCID を検索するには、「show flogi auto-area-list」コマンドと「show fcdomain fcid persistent」コマンドを使用します。

例：

```
「show flogi auto-area-list」
Fcid area allocation company id info:
<...>
   00:14:5E
   00:1B:32
   00:50:2E
   00:E0:69
   00:E0:8B
```

```
「show fcdomain fcid persistent」{OUI 00:E0:8B 用に予約されているエリア全体}

102    21:01:00:1b:32:2f:7f:63    0x020003    SINGLE FCID     YES    DYNAMIC
102    21:00:00:1b:32:0f:7f:63    0x020004    SINGLE FCID     YES    DYNAMIC

102    21:00:00:e0:8b:89:a7:07    0x021c00    ENTIRE AREA     YES    DYNAMIC
102    21:00:00:e0:8b:88:e9:22    0x024300    ENTIRE AREA     YES    DYNAMIC
```

FCID が十分にない場合は、「purge fcdomain」コマンドを使用して、指定した VSAN のダイナミック FC ID と未使用の FC ID を消去できます。

例：

```
switch#purge fcdomain fcid vsan <vsan-id>
```

ポートはすぐにアップします。

また、HBA が S_ID != 0x0 でログインしようとしている可能性もあります。

これが起こった場合に、永続性テーブルに HBA の WWN に対応するエントリがないときは、HBA で使用されている S_ID をその HBA 自体に割り当ててみます。

S_ID がすでに使用されているか、間違ったドメインに属する場合は、fcdomain によって要求が拒否されます。数回再試行した後、ポートが一時停止します。

このモードになった HBA は、FCID 空間にあるすべての FCID（0x00.00.01 から、最大ですべての 0xDD.AA.PP 番号まで）を使用してログインを試みます。

この動作は「show flogi internal event-history msgs」で確認できます。

「show flogi internal event-history msgs」（HBA がさまざまな FCID を使用してログインを試みています）

例：

```
841) Event:E_FLOGI_LRX, length:20, at 56079 usecs after Tue Jun 22 15:40:59 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  FCID: 0x000032
```

```
886) Event:E_FLOGI_RX, length:20, at 897472 usecs after Tue Jun 22 15:40:58 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  FCID: 0x000030

888) Event:E_FLOGI_FAIL, length:20, at 884758 usecs after Tue Jun 22 15:40:58 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  ev_id: 21
    rjt reason: 7 OPC: MTS_OPC_DM_GET_FCIDS(275)

903) Event:E_FLOGI_RX, length:20, at 835015 usecs after Tue Jun 22 15:40:58 2010
    WWN: 21:01:00:1b:32:af:d6:8c  VSAN: 1  ifindex: fc2/1  FCID: 0x00002f
```

この場合の解決方法は、次の例に示すように、永続性テーブルに HBA の WWN に対応するエントリを手動で設定することです。その他に、デバイスの電源を再投入するという方法もあります。こうすると通常、HBA はまず S_ID=0x0 を使用した通常の FLOGI を実行します。

例：

```
switch# conf t
switch(config)# fcdomain fcid database
switch(config-fcid-db)# vsan <vsan-id> wwn 50:05:08:b2:00:71:c8:c2 fcid 0x6fee00 area
```

それでも問題が解決しない場合は、次のコマンドを使用して、詳細な分析に役立つ情報を収集します。

```
Show tech-support flogi
Show tech-support fcdomain
Show logging log
show port internal info interface fc slot/port
show port internal event-history interface fc slot/port
show tech-support detail > bootflash:showtechdet
Capture debug flogi & debug fcdomain via following below steps:
switch# debug logfile flogi_fcdomain
switch# debug flogi all
switch# debug fcdomain all

switch(config)# int fc slot/port
switch(config-if)# shut
switch(config-if)# no shut
switch(config-if)# undebug all
switch# dir log:  {check if you have the file in log: directory}
         31     Aug 03 13:45:13 2010  dmesg
      55941     Aug 05 07:21:15 2010  flogi_fcdomain

switch# copy log:flogi_fcdomain ftp://x.y.z.w {or use tftp/scp/sftp}
```

ファイバ チャネル ノードの古い FCNS エントリがある

ファイバ チャネル ノードは SAN ファブリックにログイン（FLOGI）できますが、それらのノードの FCNS エントリが不完全です。サーバはそれらのターゲットに到達できません。

その結果、FCNS データベースで「fc4-types:fc4_features」が空になります。

考えられる原因

Nexus 5000 シリーズ スイッチが NPV コア（NPIV を装備）として設定され、レガシー ゲートウェイ スイッチに接続されたトポロジにおいて、ファイバ チャネル ノードが自身の FC4 タイプと FC4 機能を FCNS データベースに登録していない可能性があります。fc4-types:fc4_features を確認するには、次の例に示すように、「show fcns database detail」コマンドを使用します。

例：

```
switch# show fcns da fcid 0x621400 detail vsan 2
------------------------
```

```
VSAN:2     FCID:0x621400
------------------------
port-wwn (vendor)           :21:01:00:1b:32:a3:d7:2c
                             [z7095ib-1_T]
node-wwn                    :20:01:00:1b:32:a3:d7:2c
class                       :3
node-ip-addr                :0.0.0.0
ipa                         :ff ff ff ff ff ff ff ff
fc4-types:fc4_features      :
symbolic-port-name          :
symbolic-node-name          :
port-type                   :N
port-ip-addr                :0.0.0.0
fabric-port-wwn             :20:d9:00:0d:ec:e0:0e:80
hard-addr                   :0x000000
permanent-port-wwn (vendor) :20:11:00:05:1e:06:da:ea
Connected Interface         :fc2/2
Switch Name (IP address)    :N5K (10.200.220.13)
```

レガシー ゲートウェイ スイッチの中には、スイッチの FCID のエリア部分と、そのポートを通じてログインされたすべてのブレードの FCID のエリア部分が同じでなければならないものがあります。

しかし、Qlogic HBA に関する古い問題が原因で、Cisco Nexus 5000 ドメイン サーバは、デフォルトである特定の OUI と一致する Qlogic HBA に対してそれぞれ異なるエリアを割り当てます。したがって、レガシー ゲートウェイの要件とシスコのドメイン割り当て方式の間に競合が起こります。シスコは、現場で使用されている既存の古い Qlogic HBA をサポートするため、引き続きこの方式をサポートします。

解決方法

まず、使用しているすべての Qlogic OUI について「no fcid-allocation area company <oui>」を設定します（今後、フラットな FCID 割り当てが行われるようにします）。次に、影響を受けるすべてのブレードを強制的にファブリックからログアウトさせ、すでに作成された永続的 FCID エントリを Nexus 5000 スイッチ コンフィギュレーションから削除します。最後に、ブレードに再度ログインさせます。

次の「show flogi database」の出力例では、すべてのデバイスが一意のエリア ID（x01、x08、x0c）を取得しています。

例：

```
Fc2/1    2     0x620104  20:10:00:05:1e:5e:6a:85 10:00:00:05:1e:5e:6a:85
Fc2/1    2     0x620800  21:01:00:1b:32:a3:c0:2e 20:01:00:1b:32:a3:c0:2e
Fc2/1    2     0x620c00  21:01:00:1b:32:33:8b:8e 20:01:00:1b:32:33:8b:8e
```

レガシー スイッチに特有のエリア ID 要件のため、最後の 2 つのブレードもエリアを x01 にする必要があります。次の手順に従って、Qlogic アダプタを強制的に再ログインさせて 0x6201xx の範囲内の FCID が取得されるようにします。

ステップ 1　この状況にある OUI と一致するすべての WWN について、今後の FCID 割り当て方式がフラットになるよう設定（強制）します。

```
switch(configure)# no fcid-allocation area company 0x001B32
```

ステップ 2　再設定中の FCID を強制的にファブリックからログアウトさせます。

（注）　単に、そのサーバのプライマリ アップリンクとして機能している Nexus 5000 インターフェイスをシャットダウンするだけでは不十分です。そうすると、別のインターフェイスを通じてログインするだけです。適切な方法は、影響を受けるブレードをシャットダウンして、WWN の FLOGI を確実に消去することです。

ステップ 3　次の例に示すように、永続的 FCID 割り当てのために自動的に作成された設定エントリを削除します。

例：

```
switch(config)# fcdomain fcid database
switch(config-fcid-db)# no vsan 2 wwn 21:01:00:1b:32:a3:c0:2e fcid 0x620800 area dynamic
```

ステップ 4　ブレードを起動して、適切な FCID が取得されるようにします。

例：

```
Fc2/1    2     0x620104  20:10:00:05:1e:5e:6a:85 10:00:00:05:1e:5e:6a:85
Fc2/1    2     0x620123  21:01:00:1b:32:a3:c0:2e 20:01:00:1b:32:a3:c0:2e
```

FC ドメイン ID の重複が原因でインターフェイスが分離される

xE ポート タイプを使用して FC スイッチに接続された（ファブリック モードの）Cisco Nexus 5000 のファイバ チャネル インターフェイスまたは SAN ポートチャネル インターフェイスが、ドメインの重複が原因で分離されます。「show logging」ログに表示される場合があるログ メッセージの例を次に示します。

例：

```
PORT-5-IF_DOWN_DOMAIN_OVERLAP_ISOLATION: Interface fc <slot/port> is down (Isolation due
to domain overlap).
%FCDOMAIN-2-EPORT_ISOLATED: %$VSAN <vsan-id>%$ Isolation of interface san-port-channel
<channel-id> (reason: domain ID assignment failure)
%FCDOMAIN-2-EPORT_ISOLATED: %$VSAN <vsan-id>%$ Isolation of interface san-port-channel
<channel-id> (reason: other side Eport indicates isolation)
```

考えられる原因

2 つのスイッチ ファブリックが結合できない可能性があります。2 台以上のスイッチを含む 2 つのファブリックが接続されている場合に、それらのファブリックが共通の割り当て済みドメイン ID を少なくとも 1 つ持ち、さらに自動再設定オプションがディセーブルになっているとき（このオプションはデフォルトでディセーブルになっています）、2 つのファブリックの接続に使用される E ポートは、ドメイン ID の重複が原因で分離されます。

ファイバ チャネル ネットワークでは、新しいスイッチが既存のファブリックに追加されると、主要スイッチによってドメイン ID が割り当てられます。ただし、2 つのファブリックが結合するときは、主要スイッチ選出プロセスによって、既存のいずれのスイッチが結合ファブリックの主要スイッチになるかが決定されます。

新しい主要スイッチの選出は次のルールに従います。

- 空でないドメイン ID リストを持つスイッチの方が、空のドメイン ID リストを持つスイッチよりも優先されます。主要スイッチは、空でないドメイン ID リストを持つファブリック内のスイッチになります。
- 両方のファブリックがドメイン ID リストを持つ場合、2 台の主要スイッチ間の優先順位はスイッチ プライオリティの設定値によって決まります。これはユーザが設定可能なパラメータです。パラメータの値が小さいほど優先順位が高くなります。
- 上記の 2 つの基準によって主要スイッチを決定できない場合は、2 台のスイッチの WWN によって主要スイッチが決定されます。WWN の値が小さいほどスイッチ プライオリティが高くなります。

解決方法

FC ドメイン ID の重複を解決するには、分離されたスイッチ用の新しいスタティック ドメイン ID を手動で設定して重複するスタティック ドメイン ID を変更するか、スタティックなドメイン割り当てをディセーブルにして、ファブリック再設定後にスイッチが新しいドメイン ID を要求するようにします。

NX-OS CLI を使用してスタティック ドメイン ID を割り当てるには

VSAN 内のスイッチに接続されたデバイスはすべて、新しいドメイン ID が割り当てられるときに新しい FC ID を取得します。ホストまたはストレージ デバイスの FC ID が変更された場合、一部のホストまたはストレージ デバイスが期待どおりに機能しない可能性があります。

CLI を使用して FC ドメイン ID の重複を確認し、新しいドメイン ID を再割り当てするには、次の手順を実行します。

ステップ 1　「show interface fc <slot/port>」コマンドを実行して、E ポートの分離エラー メッセージを表示します。

例：

```
switch(config)# show int fc 2/2
fc2/2 is down (Isolation due to domain other side eport isolated)
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:42:00:0d:ec:d5:fe:00
    Admin port mode is E, trunk mode is off
    snmp link state traps are enabled
    Port vsan is 3
```

「show interface san-port-channel <channel-id>」コマンドを実行して、特定の VSAN の分離エラーを表示します。

例：

```
switch(config)# show interface san-port-channel 200
san-port-channel 200 is trunking (Not all VSANs UP on the trunk)
    Hardware is Fibre Channel
    Port WWN is 24:c8:00:0d:ec:d5:a3:80
    Admin port mode is auto, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,200)
    Trunk vsans (up)                       (1)
    Trunk vsans (isolated)                 (200)
    Trunk vsans (initializing)             ()
```

ステップ 2　「show fcdomain domain-list vsan <vsan-id>」コマンドを使用して、現在ファブリック内にあるドメインを表示します。

例（ドメイン ID 44 の重複が原因でスイッチが分離されています）：

```
switch(config)# show fcdomain domain-list vsan 3

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x2c(44)    20:03:00:0d:ec:3f:a5:81 [Local] [Principal]

switch(config)# show fcdomain domain-list vsan 3

Number of domains: 1
Domain ID              WWN
---------    -----------------------
```

```
 0x2c(44)    20:03:00:0d:ec:d5:fe:01 [Local] [Principal]
```

SAN ポートチャネル インターフェイスの下の特定の VSAN で分離が発生している場合は、次の例に示すように、「show port internal info interface san-port-channel <channel-id> vsan <vsan-id>」を使用してエラーを表示できます。

例：

```
switch(config)# show port internal info interface san-port-channel 200 vsan 200

  san-port-channel 200, Vsan 200 - state(down), state reason(Isolation due to domain other
side eport isolated), fcid(0x000000)
    port init flag(0x10000),  num_active_ports (2),
    Lock Info: resource [san-port-channel 200, vsan 200]
      type[0] p_gwrap[(nil)]
          FREE @ 159645 usecs after Thu Aug  5 13:35:00 2010
      type[1] p_gwrap[(nil)]
          FREE @ 159964 usecs after Thu Aug  5 13:35:00 2010
      type[2] p_gwrap[(nil)]
          FREE @ 450507 usecs after Tue Aug  3 14:14:08 2010
    0x50c8efc7
current state [TE_FSM_ST_ISOLATED_DM_ZS]
    RNID info not found.
    first time elp: 0
    Peer ELP Revision: 3
```

ステップ 3　「fcdomain domain domain-id [static | preferred] vsan vsan-id」コマンドを使用して、重複しているいずれかのドメイン ID のドメイン ID を変更します。

- static オプションを指定すると、スイッチはその特定のドメイン ID を要求します。その特定のアドレスを取得できない場合は、ファブリックから分離されます。
- preferred オプションを指定すると、スイッチは指定されたドメイン ID を要求します。その ID を取得できない場合は、別の ID を受け入れます。

ステップ 4　「fcdomain restart vsan」コマンドを使用して、Domain Manager を再起動します。

static オプションは、中断再起動または非中断再起動後の実行時に適用できますが、preferred オプションは中断再起動後の実行時にだけ適用できます。

（注）　ドメイン ID の再起動は中断的です。そのドメインにログインしていたファイバ チャネル ノードはいったんログアウトし、再びログインします。中断再設定が発生すると、データ トラフィックが影響を受けることがあります。

ファブリック再設定後にダイナミック ドメイン ID を割り当てるには

ファブリック再設定を使用してドメイン ID を再割り当てし、ドメイン ID の重複を解決できます。ファブリックを接続する前に両方のスイッチで auto-reconfigure オプションをイネーブルにした場合、中断再設定（RCF）が発生します。RCF が発生すると、新しい主要スイッチ選出が自動的に強制実行され、新しいドメイン ID が異なるスイッチに割り当てられます。

NX-OS CLI でファブリック再設定を使用して特定の VSAN 用のドメイン ID を再割り当てするには、次の手順を実行します。

ステップ 1　「show fcdomain domain-list」コマンドを使用して、スイッチにドメイン ID がスタティックに割り当てられているかどうかを確認します。

ステップ 2　ドメイン ID がスタティックに割り当てられている場合は、「no fcdomain domain」コマンドを使用してスタティックな割り当てを解除します。

ステップ 3　「show fcdomain vsan <vsan-id>」コマンドを使用して、RCF 拒否オプションがイネーブルになっているかどうかを確認します。

例：

```
switch# show fcdomain vsan 3
The local switch is the Principal Switch.

Local switch run time information:
        State: Stable
        Local switch WWN:    20:03:00:0d:ec:d5:fe:01
        Running fabric name: 20:03:00:0d:ec:d5:fe:01
        Running priority: 128
        Current domain ID: 0x2c(44)

Local switch configuration information:
        State: Enabled
        FCID persistence: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 20:01:00:05:30:00:28:df
        Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x2c(44) (preferred)

Principal switch run time information:
        Running priority: 128
Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/2               Isolated         Enabled
----------------    -------------    ------------
```

ステップ 4　rcf-reject オプションがイネーブルになっている場合は、interface コマンドを使用してから、インターフェイス モードで「no fcdomain rcf-reject vsan <vsan-id>」コマンドを使用します。

例：

```
switch(config)# interface fc 2/2
switch(config-if)# no fcdomain rcf-reject vsan 3
switch(config-if)#
```

ステップ 5　両方のスイッチで、EXEC モードで「fcdomain auto-reconfigure vsan <vsan-id>」コマンドを使用して、Domain Manager の再起動後に auto-reconfiguration がイネーブルになるようにします。

ステップ 6　「fcdomain restart vsan <vsan-id>」コマンドを使用して、Domain Manager を再起動します。

これは中断操作/中断再設定であり、データ トラフィックが影響を受けることがあります。

シスコ ファブリック サービス

ここでは、Cisco Fabric Service（CFS; シスコ ファブリック サービス）のトラブルシューティングの概要を示し、一般的な問題とその解決方法について説明します。

概要

CFS の問題をトラブルシューティングする際は、まず次のことを確認します。

- 影響を受けるすべてのスイッチで、同じアプリケーションについて CFS がイネーブルになっていることを確認します。
- 影響を受けるすべてのスイッチで、同じアプリケーションについて CFS 配信がイネーブルになっていることを確認します。

  CFS リージョン機能を使用している場合は、影響を受けるすべてのスイッチでアプリケーションが同じリージョンにあることを確認します。
- アプリケーションの保留中の変更がないこと、および CFS がイネーブルになっているアプリケーションのすべての設定変更について CFS コミットが発行されたことを確認します。
- 予期しない CFS ロック済みセッションがないことを確認します。

  予期しないロック済みセッションがある場合はクリアします。

CLI を使用した CFS の確認

CLI を使用して CFS を確認するには、次の手順を実行します。

ステップ 1　デフォルトでは、CFS 配信はイネーブルに設定されています。アプリケーションは、ファブリック内のアプリケーションが存在するすべての CFS 対応スイッチにデータと設定情報を配信できます。これが通常の動作モードです。スイッチでの CFS 配信のステートを確認するには、「show cfs status」コマンドを実行します。

例：

```
switch(config)# show cfs status
Distribution : Enabled
Distribution over IP : Enabled - mode IPv4
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled

switch(config)# show cfs merge status name rscn
```

ステップ 2　アプリケーションが一覧表示され、イネーブルになっていることを確認するには、すべてのスイッチで「show cfs application」コマンドを実行します。

例：

```
switch# show cfs application

----------------------------------------------
 Application    Enabled   Scope
----------------------------------------------
 fwm            Yes       Physical-eth
 ntp            No        Physical-fc-ip
 stp            Yes       Physical-eth
 fscm           Yes       Physical-fc
 role           No        Physical-fc-ip
 rscn           No        Logical
 radius         No        Physical-fc-ip
 fctimer        No        Physical-fc
 syslogd        No        Physical-fc-ip
 callhome       No        Physical-fc-ip
 fcdomain       No        Logical
```

```
 device-alias   Yes       Physical-fc

Total number of entries = 12
```

（注） Physical スコープは、そのアプリケーションの設定がスイッチ全体に適用されることを意味します。Logical スコープは、そのアプリケーションの設定が特定の VSAN に適用されることを意味します。

ステップ 3　ある特定のアプリケーションが CFS に登録されているスイッチのセットを確認します。物理スコープ アプリケーションでは「show cfs peers name application-name」コマンドを使用し、論理スコープ アプリケーションでは「show cfs peers name application-name vsan vsan-id」コマンドを使用します。

例：

```
switch# show cf peers name device-alias

Scope      : Physical-fc
--------------------------------------------------------------------------
Switch WWN              IP Address
--------------------------------------------------------------------------
20:00:00:0d:ec:da:6e:00 172.25.183.124                          [Local]
20:00:00:0d:ec:24:5b:c0 172.25.183.123
20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3
```

（注） 論理アプリケーションに対して「show cfs peers name application-name」コマンドを実行すると、すべての VSAN のピアが表示されます。

例：

```
switch(config)# show cfs peers name rscn

Scope      : Logical [VSAN 1]
------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
------------------------------------------------------------------------------
 106    20:00:00:0d:ec:da:6e:00 172.25.183.124                        [Local]
 98     20:00:00:0d:ec:24:5b:c0 172.25.183.123
 238    20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3


Scope      : Logical [VSAN 10]
------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
------------------------------------------------------------------------------
 82     20:00:00:0d:ec:da:6e:00 172.25.183.124                        [Local]
 5      20:00:00:0d:ec:50:09:00 172.25.183.42
 83     20:00:00:0d:ec:24:5b:c0 172.25.183.123

Total number of entries = 3


Scope      : Logical [VSAN 50]
------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
------------------------------------------------------------------------------
 66     20:00:00:0d:ec:da:6e:00 172.25.183.124                        [Local]
```

```
 28     20:00:00:0d:ec:24:5b:c0 172.25.183.123
 235    20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3


Scope      : Logical [VSAN 100]
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 90     20:00:00:0d:ec:da:6e:00 172.25.183.124                          [Local]
 100    20:00:00:0d:ec:24:5b:c0 172.25.183.123
 111    20:00:00:0d:ec:50:09:00 172.25.183.42

Total number of entries = 3
```

ステップ 4　ファブリック内のすべてのスイッチが 1 つの CFS ファブリックを構成するか、または多数の分割された CFS ファブリックを構成するかを確認するには、「show cfs merge status name application-name」コマンドと「show cfs peers name application-name」コマンドを実行して出力を比較します。2 つの出力に示されるスイッチのリストが同じである場合は、スイッチのセット全体が 1 つの CFS ファブリックを構成しています。この場合、結合ステータスはすべてのスイッチで常に「成功」になります。

例：

```
switch(config)# show cfs merge status name rscn

Logical [VSAN 1] Merge Status: Success [ Thu Aug  5 11:33:50 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 98     20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 238    20:00:00:0d:ec:50:09:00 172.25.183.42
 106    20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3


Logical [VSAN 10] Merge Status: Success [ Thu Aug  5 11:36:43 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 83     20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 5      20:00:00:0d:ec:50:09:00 172.25.183.42
 82     20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3


Logical [VSAN 50] Merge Status: Success [ Thu Aug  5 11:36:23 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 28     20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 235    20:00:00:0d:ec:50:09:00 172.25.183.42
 66     20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3
```

```
Logical [VSAN 100] Merge Status: Success [ Thu Aug  5 11:33:50 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Domain Switch WWN              IP Address
--------------------------------------------------------------------------------
 100    20:00:00:0d:ec:24:5b:c0 172.25.183.123                  [Merge Master]
 111    20:00:00:0d:ec:50:09:00 172.25.183.42
 90     20:00:00:0d:ec:da:6e:00 172.25.183.124
                                switch

Total number of switches = 3
```

「show cfs merge status name」コマンドの出力に示されるスイッチのリストが「show cfs peers name」コマンドの出力よりも短い場合、ファブリックは複数の CFS ファブリックに分割されていて、結合ステータスが「失敗」、「保留中」、「待機中」のいずれかになる場合があります。

結合の失敗のトラブルシューティング

結合時、結合するファブリック内の結合マネージャは相互にコンフィギュレーション データベースを交換します。いずれかのファブリックのアプリケーションが情報を結合し、結合が成功したかどうかを判断して、結合されたファブリック内のすべてのスイッチに結合ステータスを通知します。

結合が成功した場合、結合されたデータベースが結合ファブリック内のすべてのスイッチに配信され、新規ファブリック全体が一貫したステートになります。結合の失敗は、結合するファブリックに結合できない不整合データが含まれることを示します。

新しいスイッチをファブリックに追加した場合に、あるアプリケーションの結合ステータスが長時間「In Progress」を示すときは、いずれかのスイッチにそのアプリケーションのアクティブなセッションが存在する可能性があります。「show cfs lock」コマンドを使用して、すべてのスイッチでそのアプリケーションのロック ステータスを確認します。ロックが存在する場合、結合プロセスは進みません。変更をコミットするかセッションのロックをクリアして、結合プロセスを進めます。

（注） 結合の失敗は正しく分析する必要があります。ブランク コミットを行うスイッチを選ぶときは注意してください。小さいコンフィギュレーションによって大きいコンフィギュレーションが消去される場合があります。

CLI を使用した結合の失敗からの回復

CLI を使用して結合の失敗から回復するには、次の手順を実行します。

ステップ 1　結合の失敗を示すスイッチを特定するには、「show cfs merge status name application-name」コマンドを実行します。

例：

```
switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:47:58 2010 ]
 Local Fabric
--------------------------------------------------------------------------------
 Switch WWN              IP Address
--------------------------------------------------------------------------------
 20:00:00:0d:ec:da:6e:00 172.25.183.124                  [Merge Master]
                         switch
```

```
Total number of switches = 1

switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:43:39 2010 ]
 Local Fabric
-------------------------------------------------------------------------------
 Switch WWN              IP Address
-------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                          [Merge Master]
                         MDS-9134
 20:00:00:0d:ec:da:6e:00 172.25.183.124

Total number of switches = 2
```

ステップ 2　結合の失敗の詳細な説明を表示するには、「show cfs internal session-history name application name detail」コマンドを実行します。

例：

```
switch(config)# show cfs internal session-history name ntp
-------------------------------------------------------------------------------
Time Stamp                Source WWN              Event
User Name                 Session ID
-------------------------------------------------------------------------------
Thu Aug  5 11:45:19 2010  20:00:00:0d:ec:da:6e:00  LOCK_ACQUIRED
admin                     34684
Thu Aug  5 11:45:19 2010  20:00:00:0d:ec:da:6e:00  COMMIT[2]
admin                     34689
Thu Aug  5 11:45:20 2010  20:00:00:0d:ec:da:6e:00  LOCK_RELEASED
admin                     34684

-------------------------------------------------------------------------------
```

ステップ 3　コンフィギュレーション モードに入り、「application-name commit command」コマンドを実行してファブリック内のすべてのピアを同じコンフィギュレーション データベースに戻します。

例：

```
switch(config)# ntp commit
switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:51:02 2010 ]
 Local Fabric
-------------------------------------------------------------------------------
 Switch WWN              IP Address
-------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                          [Merge Master]
 20:00:00:0d:ec:da:6e:00 172.25.183.124
                         switch

Total number of switches = 2

switch(config)# show cfs merge status name ntp

Physical-fc-ip  Merge Status: Success [ Thu Aug  5 11:51:02 2010 ]
 Local Fabric
-------------------------------------------------------------------------------
 Switch WWN              IP Address
-------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                          [Merge Master]
                         MDS-9134
```

```
 20:00:00:0d:ec:da:6e:00 172.25.183.124

Total number of switches = 2
```

ロックの失敗のトラブルシューティング

ファブリック内で設定を配信するためには、まずファブリック内のすべてのスイッチでロックを取得する必要があります。ロックが取得されたら、コミットを実行してファブリック内のすべてのスイッチにデータを配信できます。その後でロックが解放されます。

別のアプリケーション ピアによってすでにロックが取得されている場合は、新しい設定変更をコミットできません。これは通常の状況であり、ロックが解放されるまでアプリケーションの変更を延期する必要があります。この項のトラブルシューティング手順を実行するのは、ロックが適切に解放されていないと確信される場合に限ります。

ロックは、管理者が CFS イネーブル アプリケーションの変更を設定するときに発生します。2 人の管理者が同じスイッチで同じアプリケーションを設定しようとした場合は、一方の管理者のみにロックが与えられます。もう一方の管理者は、最初の管理者が変更をコミットまたは廃棄するまで、そのアプリケーションに変更を加えることはできません。アプリケーションのロックを保持している管理者の名前を確認するには、「show cfs lock name」コマンドを使用します。ロックをクリアする前に、その管理者を確認してください。

ファブリック内の別のスイッチが CFS ロックを保持している場合もあります。「show cfs peers name」コマンドを使用して、アプリケーションの CFS 配信に参加しているすべてのスイッチを確認します。次に、各スイッチで「show cfs lock name」コマンドを使用して、そのアプリケーションの CFS ロックを所有している管理者を確認します。ロックをクリアする前に、その管理者を確認してください。CFS abort オプションを使用すると、データをファブリックに配信せずにロックが解放されます。

CLI を使用したロックの失敗に関する問題の解決

CLI を使用してロックの失敗を解決するには、次の手順を実行します。

ステップ 1　「show cfs lock name」コマンドを使用して、ロック保持者を確認します。

例：

```
switch(config)# show cfs lock name ntp

Scope      : Physical-fc-ip
--------------------------------------------------------------------------------
 Switch WWN              IP Address                  User Name    User Type
--------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42               admin        CLI/SNMP v3

Total number of entries = 1
```

ステップ 2　ロックの失敗の詳細な説明を表示するには、「show cfs internal session-history name application name detail」コマンドを実行します。

例：

```
switch(config)# show cfs internal session-history name ntp detail
--------------------------------------------------------------------------------
Time Stamp                Source WWN              Event
User Name                 Session ID
--------------------------------------------------------------------------------
Thu Aug  5 11:51:02 2010  20:00:00:0d:ec:da:6e:00  LOCK_REQUEST
```

```
admin                     35035
Thu Aug  5 11:51:02 2010  20:00:00:0d:ec:da:6e:00  LOCK_ACQUIRED
admin                     35035
Thu Aug  5 11:51:03 2010  20:00:00:0d:ec:da:6e:00  COMMIT[2]
admin                     35040
Thu Aug  5 11:51:03 2010  20:00:00:0d:ec:da:6e:00  LOCK_RELEASE_REQUEST
admin                     35035
Thu Aug  5 11:51:03 2010  20:00:00:0d:ec:da:6e:00  LOCK_RELEASED
admin                     35035
Thu Aug  5 12:03:18 2010  20:00:00:0d:ec:50:09:00  REMOTE_LOCK_REQUEST
admin                     284072
Thu Aug  5 12:03:18 2010  20:00:00:0d:ec:50:09:00  LOCK_OBTAINED
admin                     284072
```

ステップ 3　リモート ピアがロックを保持している場合は、そのスイッチで「application-name commit」コマンドまたは「application-name abort」コマンドを実行する必要があります。

例：

application-name commit コマンドの例を次に示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp commit
switch(config)#
```

例：

application-name abort コマンドの例を次に示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp abort
switch(config)#
```

システム ステートが不整合で、ロックが保持されている

不整合なシステム ステートは次のいずれかの場合に起こります。

- ファブリック内のすべてのスイッチでロックが保持されていない場合。
- ファブリック内のすべてのスイッチでロックが保持されているが、スイッチを保持しているロックを持つセッションが存在しない場合。

どちらの場合でも、clear オプションを使用してロックを解放する必要があります。

CLI を使用したロックのクリア

リモート ピアでロックが保持されていて、「application-name commit」コマンドまたは「application-name abort」コマンドを実行してもロックがクリアされないときは、「clear application-name session」コマンドを使用してファブリック内のすべてのロックをクリアします。すべてのロックがクリアされた後、ファブリック内のすべてのスイッチを同じステートに戻すために新しい配信を開始する必要があります。

例：

```
switch# clear ntp session
switch# config terminal
switch(config)# ntp commit
switch(config)#
```

配信ステータスの確認

アプリケーションを設定して変更をコミットした後、ファブリックまたは VSAN 全体に設定変更が配信されたかどうかを確認できます。

CLI を使用した配信の確認

「show cfs lock name application-name」コマンドを使用して、ファブリックで配信が進行中であるかどうかを確認します。該当するアプリケーションが出力に表示されない場合、配信は完了しています。

例：

```
switch(config)# show cfs lock name ntp

Scope      : Physical-fc-ip
------------------------------------------------------------------------------
 Switch WWN              IP Address                  User Name    User Type
------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42               admin        CLI/SNMP v3

Total number of entries = 1
```

CFS リージョンのトラブルシューティング

CFS リージョンには次のルールが適用されます。

- CFS リージョンを使用しているとき、特定のスイッチ上のアプリケーションは同時に 1 つのリージョンにのみ属することができます。
- CFS リージョンは、物理スコープ内のアプリケーションにのみ適用できます。アプリケーションの論理スコープで CFS リージョンを作成することはできません。
- アプリケーションへのリージョンの割り当ては、配信においてその初期物理スコープよりも優先されます。
- CFS リージョンの設定は、登録解除されたアプリケーション（条件付きサービス）または現在ロックされている物理スコープ アプリケーションについてはサポートされません。
- ユーザ設定に使用できるリージョンの範囲は 1 ～ 200 です。201 ～ 255 のリージョンは予約されており、ユーザ設定には使用できません。

配信の失敗

ある CFS リージョンにおけるすべてのスイッチへの設定配信の失敗を解決するには、次の手順を実行します。

ステップ 1　アプリケーションの配信がイネーブルになっていることを確認します。詳細については、「概要」（P.33）を参照してください。

ステップ 2　すべてのスイッチで、アプリケーションが同じリージョンにあることを確認します。

各スイッチで CLI を使用して、「show cfs application name application-name」コマンドを実行します。

例（device-alias アプリケーションの場合）：

```
switch(config)# show cfs lock name ntp
```

```
Scope      : Physical-fc-ip
--------------------------------------------------------------------------------
 Switch WWN              IP Address                    User Name    User Type
--------------------------------------------------------------------------------
 20:00:00:0d:ec:50:09:00 172.25.183.42                 admin        CLI/SNMP v3

Total number of entries = 1
```

例（アプリケーションが結合可能で、デフォルト リージョンにある場合）：

```
switch(config)# sho cfs application name device-alias

 Enabled        : Yes
 Timeout        : 20s
 Merge Capable  : Yes
 Scope          : Physical-fc
 Region         : Default
```

例（アプリケーションが結合可能で、リージョン 1 にある場合）：

```
switch# show cfs application name device-alias
Enabled : Yes
Timeout : 20s
Merge Capable : Yes
Scope : Physical-fc
Region : 1
```

条件付きサービスのリージョン

条件付きサービスがダウンすると（CFS から登録解除されると）、そのリージョン設定が失われます。同じ条件付きサービスが再起動されると、自動的にデフォルト リージョンに配置されます。この状況を回避するには、条件付きサービスを再起動する前に適切なリージョン情報を再設定します。

リージョンの変更

アプリケーションをあるリージョンから別のリージョンに移動した場合、結合しようとしたときにデータベースの不一致が起こることがあります。この不一致を特定して解決するには、「結合の失敗のトラブルシューティング」（P.36）を参照してください。

（注）　アプリケーションをあるリージョンから別のリージョン（デフォルト リージョンを含む）に移動すると、そのアプリケーションのすべての履歴が失われます。

VSAN

ここでは、VSAN のトラブルシューティングの概要を示し、一般的な問題とその解決方法について説明します。

概要

VSAN に関するほとんどの問題は、VSAN 実装のベスト プラクティスに従うことで回避できます。

ただし、必要であれば、Fabric Manager のファブリック分析ツールを使用して、VSAN、ゾーン分割、FCdomain、管理に関する問題、スイッチ固有の問題、ファブリック固有の問題などのさまざまなカテゴリの問題を確認できます。

Fabric Manager にはコンフィギュレーション整合性チェック ツールがあります。

[Fabric Configuration] オプションを使用してスイッチのコンフィギュレーションを分析するには、次の手順を実行します。

ステップ 1　Fabric Manager のツール メニューから、[Health] > [Fabric Configuration] をクリックします。

[Fabric Configuration Analysis] ダイアログボックスが表示されます。

ステップ 2　選択したスイッチを別のスイッチと比較するか、またはポリシー ファイルと比較するかを決定します。

- 選択したスイッチを別のスイッチと比較するには、[Policy Switch] を選択し、スイッチのドロップダウン リストからスイッチを選択します。
- ポリシー ファイルと比較するには、[Policy File] を選択し、右側のボタンをクリックしてファイル システム上のポリシー ファイル（*.XML）を選択します。

ステップ 3　[Rules] をクリックし、Fabric Configuration Analysis ツールの実行時に適用するルールを設定します。

[Rules] ウィンドウが表示されます。

ステップ 4　必要に応じて既存のルールを変更し、[OK] をクリックします。

ステップ 5　[Compare] をクリックし、コンフィギュレーションを比較します。

分析結果が表示されます。

ステップ 6　[Resolve] 列で、解決する問題をクリックします。

ステップ 7　[Resolve Issues] をクリックし、特定された問題を解決します。

ステップ 8　[Clear] をクリックし、ウィンドウの内容を消去します。

ステップ 9　[Close] をクリックし、操作を終了してウィンドウを閉じます。

コンフィギュレーション整合性チェック ツールの詳細については、『*Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 5.x*』を参照してください。

（注）　VSAN を一時停止または削除するときは、一度に 1 つの VSAN を一時停止および一時停止解除するよう注意してください。vsan suspend コマンドを実行した後、別のコンフィギュレーション コマンドを実行するときは、60 秒以上待ってください。60 秒以上待たないと、一部のファイバ チャネル インターフェイス、または PortChannel のメンバー ポートが一時停止または errdisable になる場合があります。

SAN の問題のトラブルシューティングでは、個々のデバイスの設定と接続、および SAN ファブリック全体のステータスに関する情報を収集する必要があります。

VSAN のトラブルシューティング操作

Fabric Manager でよく使うトラブルシューティング ツール

Fabric Manager で VSAN を確認するには、次の手順を実行します。

- [Information] ペインに VSAN の設定を表示するには、[Fabricxx] > [VSANxx] を選択します。
- VSAN のメンバーを表示するには、[Fabricxx] > [VSANxx] を選択してから、[Information] ペインの [Host] または [Storage] タブを選択します。
- [Information] ペインに FC ドメインの設定を表示するには、[Fabricxx] > [VSANxx] > [Domain Manager] を選択します。

トラブルシューティングによく使う CLI コマンド

VSAN、FC ドメイン、および FSPF の情報を表示するには、次の CLI コマンドを使用します。

```
show vsan
show vsan vsan-id
show vsan membership
show interface fc slot/port trunk vsan-id
show vsan-id membership
show vsan membership interface fc slot/port
```

チェックリスト

次のことを確認します。

- VSAN 内のスイッチのドメイン パラメータを確認します。
- 問題のあるポートまたは VSAN の物理接続を確認します。
- 両方のデバイスがネーム サーバにあることを確認します。
- 両方のエンド デバイスが同じ VSAN にあることを確認します。
- 両方のエンド デバイスが同じゾーンにあることを確認します。

Nexus 5000 トランク ポートがアップストリーム SAN スイッチに接続しない

Nexus 5000 トランク ポートがアップストリーム SAN スイッチに接続しないことを示す状況は、次のとおりです。

- アップストリーム スイッチに接続されたトランク ポートのステータスが「isolated」になります。
- スイッチポート トランク モードは両側でイネーブルになっています。
- 物理的なケーブル配線には問題はありません。
- ポートは両方のスイッチでアップしています。

次の例に示すように、インターフェイスのステートを調べ、インターフェイスの状況を照会することで、この問題が明らかになります。

例：

```
switch(config-if)# sho interf brief
```

```
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)

fc2/3      1      E      on      isolated         swl    --           --

switch(config-if)# show interface fc 2/3
fc2/3 is down (Isolation due to no common vsans with peer on trunk)
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:43:00:0d:ec:da:6e:00
    Admin port mode is E, trunk mode is on
```

考えられる原因

両方のインターフェイスの VSAN 許可リストが同じではありません。具体的には、両方のインターフェイスで許可されている共通の VSAN がありません。

これは次のことが原因で起こる場合があります。

- 両方のスイッチに共通の VSAN がない。
- トランクで許可されている VSAN のメンバーに共通のメンバーが含まれていない。

この例では、Nexus 5000 と MDS の FC インターフェイス上のトランク VSAN 許可リストが一致していません。

解決方法

接続されたポートを確認し、両方の FC インターフェイスについてトランクで許可される VSAN を解決します。

例：

```
switch(config-if)# show run interface fc 2/3

!Command: show running-config interface fc2/3
!Time: Wed Aug  4 16:06:04 2010

version 4.2(1)N1(1)

interface fc2/3
  switchport mode E
  switchport trunk allowed vsan 1
  no shutdown

switch(config-if)# show run interface fc 1/1

!Command: show running-config interface fc1/1
!Time: Wed Aug  4 16:20:07 2010

version 5.0(1a)

interface fc1/1
  switchport rate-mode dedicated
  switchport mode E
  switchport trunk allowed vsan 100
  no shutdown

switch(config-if)# interface fc 2/3
switch(config-if)# switchport trunk allowed vsan
add   all
switch(config-if)# switchport trunk allowed vsan add 100
switch(config-if)# show run interface fc 2/3
```

```
!Command: show running-config interface fc2/3
!Time: Wed Aug  4 16:07:25 2010

version 4.2(1)N1(1)

interface fc2/3
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 100
  no shutdown

switch(config-if)# switchport trunk allowed vsan add 1
switch(config-if)# show run interface fc 1/1

!Command: show running-config interface fc1/1
!Time: Wed Aug  4 16:20:54 2010

version 5.0(1a)

interface fc1/1
  switchport rate-mode dedicated
  switchport mode E
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 100
  no shutdown

fc2/3 is trunking
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:43:00:0d:ec:da:6e:00
    Peer port WWN is 20:01:00:0d:ec:24:5b:c0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 4 Gbps
    Transmit B2B Credit is 250
    Receive B2B Credit is 16
    Receive data field Size is 2112
    Beacon is turned off
    Trunk vsans (admin allowed and active) (1,100)
    Trunk vsans (up)                       (1,100)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()

switch(config-if)# show interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                 (Gbps)

fc2/3      1      E      on      trunking         swl    TE      4    --
```

Nexus 5000 E ポート（非トランキング）がアップストリーム SAN スイッチに接続しない

Nexus 5000 E ポートがアップストリーム SAN スイッチに接続しないことを示す状況は、次のとおりです。

- 相互接続された非トランキング E ポートのステータスを調べると、ステータスはアップになっています。ただし、すべてのファイバ チャネル サービスがスイッチ間で機能していません。
- どちらのスイッチでも、同じ VSAN 内のデバイスが FCNS データベースに表示されません。
- show topology コマンドでピア スイッチ情報が表示されません。
- ゾーンでは、メンバーがログインしていないと表示されます。

例：

```
switch(config-vsan-db)# show interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc2/4      50     E      off     up               swl    E       2    --

switch(config-if)# sho interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc1fc1/2      100    E      off     up              swl    E       2    --
```

FC トポロジは有効なピア インターフェイスを示しません。

例：

```
switch(config-if)# show topo

FC Topology for VSAN 100 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address
--------------------------------------------------------------------------------
            fc1/2  0x42(66)      Port 65795   ::

The zoneset shows one member is not active

switch(config-vsan-db)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
    pwwn 20:00:00:25:b5:00:20:0e [Host]
  * fcid 0x5a0000 [pwwn 50:0a:09:81:86:78:39:66] [Storage]

switch(config-if)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
    pwwn 50:0a:09:81:86:78:39:66 [Storage]
```

ストレージとホストは正しい VSAN に属しています。

例：

```
switch(config-vsan-db)# show flogi database vsan 100
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc2/2            100   0x5a0000  50:0a:09:81:86:78:39:66 50:0a:09:80:86:78:39:66
                         [Storage]

switch(config-if)# show flogi database vsan 100
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc4/2            100   0x640114  20:00:00:25:b5:00:20:0e 20:00:00:25:b5:02:02:09
                         [Host]
```

考えられる原因

このエラーは、「show interface brief」コマンドと「show vsan membership」コマンドによって表示されます。これらのコマンドは、一方のスイッチの E ポートが間違った VSAN に属していることを示します。

一方のスイッチの非トランキング E ポートが間違った VSAN に属しています（VSAN 100 が正しい VSAN です）。

例：

```
switch(config-if)# sho interface brief

--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                 Mode   Trunk                          Mode  Speed  Channel
                        Mode                                 (Gbps)
--------------------------------------------------------------------------------
fc1fc1/2   100    E      off     up               swl    E       2    --
```

解決方法

非トランキング E ポートを VSAN 100 に移動します。

例：

```
switch(config-vsan-db)# vsan 100 interface fc 2/4
Traffic on fc2/4 may be impacted. Do you want to continue? (y/n) [n] y
```

これでゾーンセットがアクティブになり、FC トポロジが正しくなります。

例：

```
switch(config-if)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
  * fcid 0x5a0000 [pwwn 50:0a:09:81:86:78:39:66] [Storage]
switch(config-if)# show topology

FC Topology for VSAN 100 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address
--------------------------------------------------------------------------------
            fc1/2  0x5a(90)            fc2/4  172.25.183.124
```

ホストとストレージ デバイス間の通信の問題

ホストとストレージ デバイス間の通信の問題を示す状況は、次のとおりです。

- ゾーンはアクティブです。
- ホストとストレージの両方が SAN にログインしています。
- ストレージ ポートがアクティブ ゾーンセットにログインしていません。

例：

```
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
    pwwn 50:0a:09:81:86:78:39:66 [Storage]
```

考えられる原因

ホストまたはストレージ ポートが間違った VSAN に属しています。

例：

```
switch(config)# show fcns database

VSAN 50:
------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
------------------------------------------------------------------------
0x420000    N     50:0a:09:81:86:78:39:66 (NetApp)        scsi-fcp:target
                  [Storage]
```

解決方法

ストレージ ポートを正しい VSAN に移動します（この例では、VSAN 100 が正しい VSAN です）。

例：

```
switch(config)# show flogi database vsan 50
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc2/2            50    0x420000  50:0a:09:81:86:78:39:66 50:0a:09:80:86:78:39:66
                           [Storage]

Total number of flogi = 1.

switch(config)# vsan database
switch(config-vsan-db)# vsan 100 interface fc 2/2
Traffic on fc2/2 may be impacted. Do you want to continue? (y/n) [n] y
switch(config-vsan-db)# show zoneset active vsan 100
zoneset name ZoneSet_Host_Storage vsan 100
  zone name Zone_Host_Storage vsan 100
  * fcid 0x640114 [pwwn 20:00:00:25:b5:00:20:0e] [Host]
  * fcid 0x5a0000 [pwwn 50:0a:09:81:86:78:39:66] [Storage]
```

スイッチ間の VSAN がダウンしている

スイッチ間の VSAN がダウンしている問題を示す状況は、次のとおりです。

- 両方のスイッチで VSAN が設定されています。
- トランク許可リストによってその VSAN が許可されています。

- VSAN がダウンしている（初期化ステート）と報告されます。
- ゾーンはアクティブです。
- ホストとストレージの両方が SAN にログインしています。

  この障害では、ストレージ ポートがアクティブ ゾーンセットにログインしていません。

次の例に示すように、インターフェイスを調べるとエラーが表示されます。

例：

```
switch(config-if)# show interface fc 2/4 trunk vsan 10
fc2/4 is trunking
    Vsan 10 is down (Isolation due to domain id assignment failure)

switch(config-if)# show port internal info interface fc 2/4 | grep Isolation
  fc2/4, Vsan 10 - state(down), state reason(Isolation due to domain id assignment
failure), fcid(0x000000)
  fc2/4, Vsan 50 - state(down), state reason(Isolation due to vsan not configured on
peer), fcid(0x000000)
```

考えられる原因

複数の VSAN に同じスタティック DomainID が設定されている可能性があります。

例：

```
switch(config-if)# show fcdomain domain-list vsan 10

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x53(83)    20:0a:00:0d:ec:da:6e:01 [Local] [Principal]

switch(config)# show fcdomain domain-list vsan 10

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x53(83)    20:0a:00:0d:ec:24:5b:c1 [Local] [Principal]
```

解決方法

いずれかの VSAN の DomainID を変更します。

例：

```
switch(config)# vsan database
switch(config-vsan-db)# vsan 10 suspend
switch(config-vsan-db)# no vsan 10 suspend
switch(config-vsan-db)# show interface fc 2/4

Number of domains: 1
Domain ID              WWN
---------    -----------------------
 0x52(82)    20:0a:00:0d:ec:da:6e:01 [Local] [Principal]

switch(config-vsan-db)# sho interface fc 2/4  | begin Trunk
    Trunk vsans (admin allowed and active) (1,10,50,100)
    Trunk vsans (up)                       (1,10,50,100)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
```

レジスタとカウンタ

物理層の問題の特定

ファイバ チャネル SFP 光ファイバに関する物理層の問題をトラブルシューティングするには、次のコマンドを使用します。

```
switch# show interface fc x/y transceiver details
```

次の例では、サポートされている速度、公称ビット レート、SFP でサポートされているリンク長などの有用な情報がコマンドの結果に含まれていることがわかります。

例：

```
switch# show interface fc 3/1 transceiver details
fc3/1 sfp is present
    name is CISCO-FINISAR
    part number is FTLF8524P2BNL-C2
    revision is 0000
    serial number is FNS0928K161
    fc-transmitter type is short wave laser w/o OFC (SN)
    fc-transmitter supports intermediate distance link length
    media type is multi-mode, 62.5m (M6)
    Supported speed is 400 MBytes/sec
    Nominal bit rate is 4300 MBits/sec
    Link length supported for 50/125mm fiber is 150 m(s)
    Link length supported for 62.5/125mm fiber is 70 m(s)
    cisco extended id is unknown (0x0)

    no tx fault, no rx loss, in sync state, Diag mon type 104
```

このコマンドは、詳細な SFP 診断情報と警告およびアラーム（存在する場合）も出力します。

例：

```
SFP Detail Diagnostics Information
  ------------------------------------------------------------------------------
                                    Alarms                  Warnings
                                 High        Low         High          Low
  ------------------------------------------------------------------------------
  Temperature  41.50 C         95.00 C    -25.00 C     90.00 C      -20.00 C
  Voltage       3.45 V          3.90 V      2.70 V      3.70 V        2.90 V
  Current       7.18 mA        17.00 mA     1.00 mA    14.00 mA       2.00 mA
  Tx Power     -4.41 dBm       -2.00 dBm  -11.74 dBm   -2.00 dBm    -11.02 dBm
  Rx Power     -4.40 dBm        1.00 dBm  -20.00 dBm   -1.00 dBm    -18.24 dBm
  Transmit Fault Count = 0
  ------------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

次に、このコマンドの出力例を 2 つ示します。最初の例は、RX 電力の下限アラームを示します。2 番目の例は、TX、RX、および電流の下限アラームを示します。2 番目の例の問題となっているインターフェイスは、ビット エラー レートが高すぎることが原因で「Error Disabled」ステートになっていました。

RX 電力の下限アラーム

```
--------------------------------------------------------------------------------
                                     Alarms                  Warnings
                                  High        Low         High          Low
--------------------------------------------------------------------------------
   Temperature  35.02 C         70.00 C      0.00 C     70.00 C        0.00 C
   Voltage       0.00 V          0.00 V      0.00 V      0.00 V        0.00 V
   Current       7.22 mA        16.00 mA     2.00 mA    14.00 mA       2.40 mA
   Tx Power     -0.57 dBm        1.00 dBm   -8.21 dBm    0.00 dBm     -7.21 dBm
   Rx Power    -18.86 dBm --     1.00 dBm  -16.58 dBm    0.00 dBm    -14.44 dBm

--------------------------------------------------------------------------------
   Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

電流、TX 電力、および RX 電力の下限アラーム

```
--------------------------------------------------------------------------------
                                     Alarms                  Warnings
                                  High        Low         High          Low
--------------------------------------------------------------------------------
   Temperature  32.75 C         70.00 C      0.00 C     70.00 C        0.00 C
   Voltage       0.00 V          0.00 V      0.00 V      0.00 V        0.00 V
   Current       0.00 mA  --    16.00 mA     2.00 mA    14.00 mA       2.40 mA
   Tx Power       N/A     --     1.00 dBm   -8.21 dBm    0.00 dBm     -7.21 dBm
   Rx Power    -22.22 dBm --     1.00 dBm  -16.58 dBm    0.00 dBm    -14.44 dBm

--------------------------------------------------------------------------------
   Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

次の例では、Twinax（銅）の詳細なトランシーバ情報は示されていないことに注意してください。

```
switch# sh interface ethernet 1/19 transceiver details
Ethernet1/19
    sfp is present
    name is Molex Inc.
    part number is 74752-1301
    revision is E
    serial number is 733010037
    nominal bitrate is 0 MBits/sec
    Link length supported for 50/125mm fiber is 0 m(s)
    Link length supported for 62.5/125mm fiber is 0 m(s)
    cisco id is --
    cisco extended id number is 4

    Invalid calibration
```

FcoE にバインドされたイーサネット インターフェイスのカウンタの表示

「show interface ethernet」コマンドには簡易版と詳細版の 2 種類があります。それぞれの例を次に示します。

簡易版

例：

（注） ジャンボ フレームが増えていることと、RX または TX ポーズ フレーム カウンタ（存在する場合）を確認してください。後者は輻輳の問題を示す場合があります。

```
switch# show interface ethernet 1/4
Ethernet1/4 is up
  Hardware: 1000/10000 Ethernet, address: 000d.ecd5.a38b (bia 000d.ecd5.a38b)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10g

  [省略]

  RX
    9507 unicast packets  918874 multicast packets  3473 broadcast packets
    931854 input packets  76225281 bytes
    7121 jumbo packets  0 storm suppression packets
    0 runts  0 giants  0 CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 Rx pause
  TX
    3986 unicast packets  294583 multicast packets  36307 broadcast packets
    334876 output packets  46873259 bytes
    1227 jumbo packets
    0 output errors  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble
    2266 Tx pause
  24 interface resets
```

詳細版

次の例では、「show interface ethernet」コマンドの詳細版の出力を分けて示しています。これには、通常トラフィックのカウンタと物理層およびプロトコル エラーのカウンタがどちらも含まれます。接続やパフォーマンスの問題があるときは常にこれらのカウンタをモニタしてください。

例：

```
switch# sh interface ethernet 1/4 counters detailed all Ethernet1/4

  64 bit counters:
   0.                      rxHCTotalPkts = 931881
   1.                       txHCTotalPks = 335522
   2.                    rxHCUnicastPkts = 9507
   3.                    txHCUnicastPkts = 3986
   4.                  rxHCMulticastPkts = 918901
   5.                  txHCMulticastPkts = 295229
   6.                  rxHCBroadcastPkts = 3473
   7.                  txHCBroadcastPkts = 36307
```

```
   8.                          rxHCOctets = 76228116
   9.                          txHCOctets = 46926647
  10.                  rxTxHCPkts64Octets = 1065359
  11.               rxTxHCpkts65to127Octets = 105246
  12.             rxTxHCpkts128to255Octets = 43798
  13.             rxTxHCpkts256to511Octets = 13822
  14.            rxTxHCpkts512to1023Octets = 30742
  15.           rxTxHCpkts1024to1518Octets = 88
  16.           rxTxHCpkts1519to1548Octets = 0
  17.                      rxHCTrunkFrames = 895722
  18.                      txHCTrunkFrames = 69387
  19.                       rxHCDropEvents = 0

All Port Counters:
   0.                             InPackets = 931881
   1.                              InOctets = 76228116
   2.                           InUcastPkts = 9507
   3.                           InMcastPkts = 918901
   4.                           InBcastPkts = 3473
   5.                          InJumboPkts = 7121
   6.                    StormSuppressPkts = 0
   7.                            OutPackets = 335522
   8.                             OutOctets = 46926647
   9.                          OutUcastPkts = 3986
  10.                          OutMcastPkts = 295229
  11.                          OutBcastPkts = 36307
  12.                         OutJumboPkts = 1227
  13.                    rxHCPkts64Octets = 889975
  14.                 rxHCPkts65to127Octets = 26702
  15.               rxHCPkts128to255Octets = 6072
  16.               rxHCPkts256to511Octets = 1913
  17.              rxHCpkts512to1023Octets = 11
  18.             rxHCpkts1024to1518Octets = 87
  19.             rxHCpkts1519to1548Octets = 0
  20.                    txHCPkts64Octets = 175384
  21.                 txHCPkts65to127Octets = 78544
  22.               txHCPkts128to255Octets = 37726
  23.               txHCPkts256to511Octets = 11909
  24.              txHCpkts512to1023Octets = 30731
  25.             txHCpkts1024to1518Octets = 1
  26.             txHCpkts1519to1548Octets = 0
  27.                           ShortFrames = 0
  28.                            Collisions = 0
  29.                             SingleCol = 0
  30.                              MultiCol = 0
  31.                               LateCol = 0
  32.                          ExcessiveCol = 0
  33.                            LostCarrier = 0
  34.                              NoCarrier = 0
  35.                                  Runts = 0
  36.                                 Giants = 0
  37.                               InErrors = 0
  38.                              OutErrors = 0
  39.                          InputDiscards = 0
  40.                          BadEtypeDrops = 0
  41.                            IfDownDrops = 0
  42.                         InUnknownProtos = 0
  43.                                txErrors = 0
  44.                                   rxCRC = 0
  45.                                  Symbol = 0
  46.                              txDropped = 0
  47.                          TrunkFramesTx = 69387
  48.                          TrunkFramesRx = 895722
  49.                             WrongEncap = 0
```

```
                          Babbles = 0
                        Watchdogs = 0
                              ECC = 0
                         Overruns = 0
                        Underruns = 0
                         Dribbles = 0
                         Deferred = 0
                          Jabbers = 0
                         NoBuffer = 0
                          Ignored = 0
                      bpduOutLost = 0
                      cos0OutLost = 0
                      cos1OutLost = 0
                      cos2OutLost = 0
                      cos3OutLost = 0
                      cos4OutLost = 0
                      cos5OutLost = 0
                      cos6OutLost = 0
                      cos7OutLost = 0
                          RxPause = 0
                          TxPause = 2266
                           Resets = 0
                          SQETest = 0
                   InLayer3Routed = 0
               InLayer3RoutedOctets = 0
                    OutLayer3Routed = 0
              OutLayer3RoutedOctets = 0
                   OutLayer3Unicast = 0
             OutLayer3UnicastOctets = 0
                 OutLayer3Multicast = 0
           OutLayer3MulticastOctets = 0
                    InLayer3Unicast = 0
              InLayer3UnicastOctets = 0
                  InLayer3Multicast = 0
            InLayer3MulticastOctets = 0
              InLayer3AverageOctets = 0
            InLayer3AveragePackets = 0
             OutLayer3AverageOctets = 0
           OutLayer3AveragePackets = 0
```

ファイバ チャネル インターフェイスのカウンタについて

「show interface」コマンドは、ファイバ チャネル インターフェイスに関する物理層またはパフォーマンスの問題をトラブルシューティングするときに非常に便利です。

このコマンドの出力では、入力/出力カウンタと入力/出力の廃棄またはエラーに注意します。

入力廃棄が増えるときは、Forwarding Information Base（FIB; 転送情報ベース）内にその FC パケットの有効なルートがありません。ルートを持たないパケットはすべて廃棄と見なされ、スーパーバイザに送信されます。これらのパケットはドロップされないことに注意してください。ただし、スーパーバイザに送信される前にポリシングされます。また、MAC ASIC にエラーがないかチェックする必要があります。

出力廃棄が増えるときは、出力が遅すぎるためにパケットが出力でタイムアウトしています。接続先のデバイスが、バッファ クレジットに応答しない、またはバッファ クレジットを補充しない低速ドレイン レシーバである可能性があるため、接続先のデバイスを確認します。この場合は、Nexus 5000 FC インターフェイスでバック プレッシャが起こります。

例：

```
switch# show interface fc2/1
fc2/1 is trunking
```

```
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:41:00:0d:ec:a4:02:80

[省略]

    1 minute input rate 5048 bits/sec, 631 bytes/sec, 9 frames/sec
    1 minute output rate 6752 bits/sec, 844 bytes/sec, 9 frames/sec
      36398816 frames input, 2422447564 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      36368010 frames output, 3213593392 bytes
        0 discards, 0 errors
      1 input OLS, 1 LRR, 0 NOS, 0 loop inits
      1 output OLS, 2 LRR, 0 NOS, 0 loop inits
      16 receive B2B credit remaining
      250 transmit B2B credit remaining
      0 low priority transmit B2B credit remaining
    Interface last changed at Thu Jan 28 18:26:30 2010
```

ファイバ チャネルの MAC に関する問題のトラブルシューティング

「show hardware」コマンドは、FC の物理層の問題をトラブルシューティングするときに非常に便利です。

```
Show hardware internal fc-mac x port y statistics
```

このコマンドの出力には、次の有用な情報が含まれます。

- 物理層の情報

  ```
  FCP_CNTR_MAC_RX_LOSS_OF_SYNC - Loss of Sync received counter
  ```

- パフォーマンスの情報

  ```
  FCP_CNTR_MAC_CREDIT_IG_XG_MUX_SEND_RRDY_REQ - Receiver Ready's Sent
  FCP_CNTR_MAC_CREDIT_EG_DEC_RRDY - Receiver Ready's Received
  ```

- クラス 3 通常トラフィックのカウンタ

  ```
  FCP_CNTR_MAC_DATA_RX_CLASS3_FRAMES
  FCP_CNTR_MAC_DATA_RX_CLASSF_FRAMES
  FCP_CNTR_MAC_DATA_RX_CLASS3_WORDS
  FCP_CNTR_MAC_DATA_RX_CLASSF_WORDS
  FCP_CNTR_MAC_DATA_TX_CLASS3_FRAMES
  FCP_CNTR_MAC_DATA_TX_CLASSF_FRAMES
  FCP_CNTR_MAC_DATA_TX_CLASS3_WORDS
  FCP_CNTR_MAC_DATA_TX_CLASSF_WORDS
  ```

- ファイバ チャネルのプリミティブ シーケンス

  ```
  FCP_CNTR_LINK_RESET_IN - Link Resets Received
  FCP_CNTR_OLS_OUT- Offline Sequences Sent
  FCP_CNTR_NOS_OUT - Not Operational Sequence Sent
  FCP_CNTR_LRR_OUT - Link Reset Responses Sent
  FCP_CNTR_LINK_FAILURE
  ```

例：

```
switch# show hardware internal fc-mac 2 port 1 statistics
 ADDRESS     STAT                                                  COUNT
__________ ________                                          ____________________
0x0000003c FCP_CNTR_MAC_RX_LOSS_OF_SYNC                                       0x5
0x0000003d FCP_CNTR_MAC_RX_BAD_WORDS_FROM_DECODER                            0xec
```

```
0x00000042 FCP_CNTR_MAC_CREDIT_IG_XG_MUX_SEND_RRDY_REQ                  0x5ec
0x00000043 FCP_CNTR_MAC_CREDIT_EG_DEC_RRDY                              0xc41
0x00000061 FCP_CNTR_MAC_DATA_RX_CLASS3_FRAMES                           0x5d2
0x00000062 FCP_CNTR_MAC_DATA_RX_CLASSF_FRAMES                            0x1a
0x00000069 FCP_CNTR_MAC_DATA_RX_CLASS3_WORDS                         0x140b14
0x0000006a FCP_CNTR_MAC_DATA_RX_CLASSF_WORDS                            0xdcc
0x00000065 FCP_CNTR_MAC_DATA_TX_CLASS3_FRAMES                           0xc24
0x00000066 FCP_CNTR_MAC_DATA_TX_CLASSF_FRAMES                            0x1d
0x0000006d FCP_CNTR_MAC_DATA_TX_CLASS3_WORDS                         0x4b9538
0x0000006e FCP_CNTR_MAC_DATA_TX_CLASSF_WORDS                            0xabc
0xffffffff FCP_CNTR_LINK_RESET_IN                                         0x2
0xffffffff FCP_CNTR_OLS_OUT                                               0x5
0xffffffff FCP_CNTR_NOS_OUT                                               0x2
0xffffffff FCP_CNTR_LRR_OUT                                               0x7
0xffffffff FCP_CNTR_LINK_FAILURE                                          0x2
```

FC のパフォーマンスの問題をトラブルシューティングするときは、R_RDY、Link Reset、Link Reset Response の各カウンタを調べます。これらのカウンタは、パフォーマンスの問題を引き起こす可能性があるバッファ ツー バッファ クレジットの問題を判別するのに役立ちます。

ファイバ チャネルの転送に関する問題のトラブルシューティング

ファイバ チャネルの転送に関する問題をトラブルシューティングするには、N5K に GATOS という MAC/転送 ASIC が搭載されていることを知っておくことが重要です。ここでは、この ASIC 専用のコマンドについて説明します。

各ファイバ チャネル インターフェイスには GATOS 番号が割り当てられるので、転送の問題を理解するには、問題になっている FC インターフェイスの GATOS 番号を特定する必要があります。

次の例について考えます。

```
switch# sh platform fwm info pif fc2/1
dump pif info: ifindex 0x1080000 dump_all 0 verbose 1
fc2/1: slot 1 port 0 state 0x0 pi_if 0x88bbb74 fwimpd ctx 0x889d4ec
fc2/1: oper_mode 0x1 rcvd_rbind: No
fc2/1: iftype 0x1  encap 0x5  bound_if? N #lifs 1 fwimpd ctx 0x88bd74c
fc2/1: lif_blk(pi) 0x8523da4 vif_id_alloc_bmp 0x887360c
fc2/1: cfg_lif_blk_size 0 lif_blk_base(pi) 1922 lif_blk_size(pi) 1
fc2/1: cfg_lif_blk_size(pi) 0
fc2/1: if_flags 0x0 num_sub_lif_tbls 0 Num HIFs pinned 0
fc2/1 pd: lif_entries 1  if_map_idx 49  if_lid 33 if_fcoe_lid 34
fc2/1 pd: reverse ifmap lookup 'same' ifmap_idx 49
fc2/1: SAT_HIF Port?: No
```

この例の次の部分で、gatos_num 13 がファイバ チャネル インターフェイス 2/1 の GATOS インスタンスであることがわかります。

```
fc2/1 pd: slot 1  logical port num 4  gatos_num 13  fwm_inst 0  fc 0
fc2/1 pd: pif_type 'data fc'(2) hw_present 1  port map idx 49
fc2/1 pd: fabric a info: voq 0-1  port_id 29 connected 1 up 1
fc2/1 pd: fabric b info: voq 0-1  port_id 29 connected 1 up 1
fc2/1 pd: subported 1 primary 1 atherton 0
fc2/1 pd: sup_src_dst_if 17  lif_blk 0-0
fc2/1 pd: policer info: uc (sel 2) mc (sel 1) bc (sel 0)
fc2/1 pd: mac-addr 000d.eca4.02b4
```

この例の次の部分で、転送のドロップおよび廃棄情報も出力されていることがわかります。

```
fc2/1 pd: tx stats: bytes 4958178736 frames 36360131 discard 0 drop 0
fc2/1 pd: rx stats: bytes 2421909296 frames 36390924 discard 0 drop 0
```

また、問題の FC インターフェイスに対応する GATOS インスタンスの GATOS エラーを表示することもできます。この例の次の部分で、このコマンドではゼロでないカウンタのみが表示されることがわかります。

```
switch# show platform fwm info gatos-errors 13
Printing non zero Gatos error registers:
DROP_FCF_SW_VSAN_IDX_MISS: res0 = 60 res1 = 0
DROP_FCF_SW_DOMAIN_IDX_MISS: res0 = 489036 res1 = 0
DROP_FCF_SW_TBL_MISS: res0 = 489036 res1 = 0
DROP_NO_FABRIC_SELECTED: res0 = 489036 res1 = 0
DROP_VLAN_MASK_TO_NULL: res0 = 489036 res1 = 0
```

上の 2 つの部分の最初の方に、ドロップと廃棄が示されています。vethernet および VFC インターフェイスではドロップ カウンタと廃棄カウンタは分かれていることに注意してください。2 番目の例の出力を見ると、ドロップの理由を関連付けるのに役立ちます。

```
switch# show platform fwm info pif ethernet 1/4
dump pif info: ifindex 0x1a003000 dump_all 0 verbose 1
Eth1/4: slot 0 port 3 state 0x0 pi_if 0x876acb4 fwimpd ctx 0x876171c
Eth1/4: oper_mode 0x100000 rcvd_rbind: No
Eth1/4: iftype 0x1  encap 0x1  bound_if? Y #lifs 1 fwimpd ctx 0x879f70c
Eth1/4: lif_blk(pi) 0x87cc9a4 foo vif_id_alloc_bmp 0x88313f4
Eth1/4:    0
Eth1/4: cfg_lif_blk_size 0 lif_blk_base(pi) 512 lif_blk_size(pi) 128
Eth1/4: cfg_lif_blk_size(pi) 0
Eth1/4: if_flags 0x0 num_sub_lif_tbls 0 Num HIFs pinned 0
Eth1/4: max_hifpc_mbrs 0, max_hif_ports 0
Eth1/4 pd: lif_entries 1  if_map_idx 8  if_lid 35 if_fcoe_lid 36
Eth1/4 pd: reverse ifmap lookup 'same' ifmap_idx 8
Eth1/4: SAT_HIF Port?: No
Eth1/4 pd: slot 0  logical port num 3  gatos_num 0  fwm_inst 0  fc 0
Eth1/4 pd: pif_type 'data eth'(1) hw_present 1  port map idx 8
Eth1/4 pd: fabric a info: voq 0-7  port_id 55 connected 1 up 1
Eth1/4 pd: fabric b info: voq 0-7  port_id 55 connected 1 up 1
Eth1/4 pd: subported 0 primary 1 atherton 0
Eth1/4 pd: sup_src_dst_if 6  lif_blk 384-511
Eth1/4 pd: policer info: uc (sel 2) mc (sel 1) bc (sel 0)
Eth1/4 pd: mac-addr 000d.ecd5.a38b
```

この例の次の部分の 2 行目にドロップが示されています。

```
Eth1/4 pd: tx stats: bytes 50256531 frames 336488 discard 0 drop 0
Eth1/4 pd: rx stats: bytes 6718252 frames 77220 discard 0 drop 845482
```

この例の次の部分で、FcoE カウンタが分かれていることがわかります。

```
Eth1/4 pd fcoe: tx stats: bytes 2927716 frames 3919 discard 0 drop 0
Eth1/4 pd fcoe: rx stats: bytes 15307492 frames 9470 discard 0 drop 0
```

この例の次の部分で、このコマンドがドロップの原因の特定に役立つことがわかります。

```
switch# show platform fwm info gatos-errors 0
Printing non zero Gatos error registers:
DROP_INGRESS_FW_PARSING_ERROR: res0 = 93 res1 = 0
DROP_SRC_VLAN_MBR: res0 = 2567226 res1 = 0
DROP_FCF_SW_DOMAIN_IDX_MISS: res0 = 2445 res1 = 0
DROP_FCF_SW_TBL_MISS: res0 = 2445 res1 = 0
DROP_NO_FABRIC_SELECTED: res0 = 2556 res1 = 0
DROP_VLAN_MASK_TO_NULL: res0 = 2556 res1 = 0
DROP_SRC_MASK_TO_NULL: res0 = 522 res1 = 0
```

CHAPTER 6

セキュリティに関する問題のトラブルシューティング

Cisco Nexus 5000 シリーズ NX-OS は、意図的な攻撃または意図しない深刻な間違いに起因する性能低下や障害、データの損失や損傷からネットワークを保護するセキュリティを提供します。

この章では、Cisco Nexus 5000 シリーズ スイッチでセキュリティに関連して発生する問題を特定し、解決する方法について説明します。

この章で説明する内容は、次のとおりです。

ロール

ユーザがログインするとロールの割り当てに失敗する

RBAC の観点から見たとき、ユーザがログインするとロールの割り当てに失敗します。

考えられる原因

TACAC+ サーバまたは RADIUS サーバで AV-Pair が適切に設定されていません。

解決方法

次の手順を実行して、ロールの割り当てを完了します。

ステップ 1 TACACS+ サーバ（ACS サーバなど）の設定を確認します。

- 次のメニュー パスを使用して、該当の設定にアクセスします。

  [Interface Configuration] > [TACACS+ (Cisco IOS)]

  - シェル（exec）の [User] ボックスを確認します。
  - Advanced TACACS+ Features を確認します。

  選択したサービスごとに、カスタマイズした TACACS 属性を詳細な設定オプションに入力するウィンドウを表示します。
- 次のメニュー パスを使用して該当の設定にアクセスし、シェル属性にストリングを追加します。

  [User Setup] >[Add/Edit "admin"] > [TACACS+ Settings]

  - シェル属性とカスタム属性のボックスを確認します。

- テキストボックスに次のストリングを追加します。

  cisco-av-pair=shell:roles="network-admin"

ステップ 2　RADIUS サーバ（ACS サーバなど）の設定を確認します。

- 次のメニュー パスを使用して該当の設定にアクセスします。

  [Network Configuration] > [AAA] > [AAA Servers] > [svi,20.1.1.2,CiscoSecure ACS]

  [Network Configuration] > [AAA] > [AAA Client] > [20.1.1.1 20.1.1.1 RADIUS (Cisco IOS/PIX 6.0)] > [SharedSecret=test1234, Authenticate Using=RADIUS (Cisco IOS/PIX 6.0)]

  [Interface Configuration] > [RADIUS (Cisco IOS/PIX 6.0)]

  - cisco-av-pair の [User] を確認します。
- 次のメニュー パスを使用して該当の設定にアクセスし、RADIUS 属性にストリングを追加します。

  [User Setup] > [Add/Edit <username>] > [Cisco IOS/PIX 6.x RADIUS Attributes]

  - 属性のボックスを確認します。
  - 次のストリングを入力します。

    shell:roles="network-admin"

ステップ 3　ユーザ アカウントで指定されている RADIUS サーバ（RADIUSD サーバなど）の設定を確認します。

- 次のパスを使用してユーザ アカウントの定義にアクセスします。

  .../etc/raddb
- ユーザ アカウントの定義に次の内容があることを確認します。

  cisco-avpair= "shell: roles = network-admin"

ステップ 4　このユーザで再度ログインします。

ステップ 5　「show user-account」コマンドを使用して、ロールの割り当てを確認します。

ロールの許可/拒否のアクションを指定するルールが正しく機能しない

ユーザ定義のロールをユーザ アカウントに割り当てると、そのロールのルール ポリシーが機能していないように見えます。たとえば、ロール設定のルールで、すべてのインターフェイス コンフィギュレーション コマンドを拒否するように設定したとします。それでも、ユーザはインターフェイスのコマンドを引き続き設定できます。

考えられる原因

ロールでのルール設定の順序が正しくありません。

（注）　RBAC パーサは、ルール番号が大きいルールから順番にアクセスします。

解決方法

正しく機能していないルールを特定し、そのルールよりも前の順番にあるルールの中に、このルールと矛盾するものやこのルールを無効にするものがないか確認します。

たとえば、正しく機能しないルールのルール ID が 10 である場合は、ルール ID が 11 以上のルールをすべて調べ、ルール 10 と矛盾するものがないか確認します。この例として、ルール 15 によってルール 10 が無効になっていることがわかったとします。この矛盾を解決するには、ルール 15 を修正するか、ルール 10 のルール ID を 16 以上の値に変更する必要があります。

ロールのインターフェイスまたは VLAN のポリシーが正しく機能していないように見える

ユーザ定義のロールをユーザ アカウントに割り当てて、特定のインターフェイスへのアクセスが拒否されるようにそのロールのインターフェイスまたは VLAN のポリシーを設定しても、そのユーザ アカウントで「show」コマンドを使用すると、アクセスが拒否されるはずのインターフェイスまたは VLAN の設定、ステータス、指定内容、または統計を引き続き表示できます。

考えられる原因

そのインターフェイスまたは VLAN のロールのポリシーを、ユーザが「show interface brief」や「show vlan」などの CLI コマンドを使用して確認しています。

解決方法

RBAC は、コマンドを表示するときのフィルタ処理には対応していません。インターフェイスや VLAN のロールのポリシーは、コンフィギュレーション コマンドまたは操作コマンドのみに適用されます。

考えられる原因

ユーザがロールに適切に割り当てられていません。

解決方法

- 「show user-account」コマンドを使用して、そのユーザへのロール割り当てを確認します。
- 「show role name <name>」コマンドを使用してロール定義を確認します。

1 人のユーザに複数のロールを割り当てると、正しく機能していないように見える

1 つのユーザ アカウントを複数のロールに割り当てて、あるコマンドへのアクセスが拒否されるようにそのいずれかのロールで設定していても、ユーザはそのコマンドにアクセスできます。その結果、複数のロールではコマンド パーサが機能していないように見えます。

考えられる原因

1 つのユーザ アカウントに割り当てた複数のロールは順番に解析されるとユーザが想定している可能性があります。

解決方法

NXOS の設計上、複数のロールは、結合して許可する機能で解析されます。たとえば、各コマンドはすべてのロールで検証され、比較されます。

いずれかのロールで許可されているコマンドをユーザが使用すれば、CLI で操作を継続できます。

たとえば、「interface eth1/1」コマンドがロールで許可されていれば、ユーザは CLI からインターフェイス eth1/1 のコンフィギュレーション モードに入ることができます。

各ロールは、それぞれのポリシー（インターフェイス、VLAN、VSAN など）を他のロールに関係なく適用します。この例のように、あるロールで eth1/1 を拒否するインターフェイス ポリシーを設定していると、そのロールではこのコマンドは拒否されますが、別のインターフェイス ポリシーを持つロールが他に存在し、そこでは同じインターフェイスが許可されていることが考えられます。

ロール設定の変更が適用されない

ユーザ アカウントをロールに割り当てた後、そのユーザが Nexus 5000 にログインしていると、そのロール設定のどのような変更もそのユーザにすぐには適用されません。

考えられる原因

ロール A に割り当てたユーザ アカウントにユーザがログインしているときに管理者がロール A を変更していますが、その管理者はロール A に対する変更がログイン中のユーザにただちに適用されると想定しています。しかし、そのユーザはロールに適切に割り当てられていません。

解決方法

NXOS では、ロール設定の変更がリアルタイムではアクティブになりません。つまり、ユーザが次にログインしたときに、新しいロールに対する設定の変更が初めて有効になります。

機能グループの削除が CLI で拒否される

管理者が「no role feature-group name <group-name>」コマンドを使用して機能グループを削除しようとすると CLI で拒否されます。

考えられる原因

その機能グループが使用中であることが CLI エラーで示されています。つまり、この機能グループを指定しているロール設定が存在します。

解決方法

このエラーを解決するには、次の手順を実行します。

- 「show role | egrep Role:|feature-group」コマンドを使用して、このロールにどの機能グループが関連付けられているか、またどのロールの下にどの機能グループが存在しているかを表示します。
- ロール コンフィギュレーション モードで「no rule」コマンドを使用して、該当の関連付けを解除します。続いて機能グループを削除します。

AAA

TACACS+ 認証や RADIUS 認証でユーザがログインできない

サーバグループを Nexus 5000 向けに適切に設定し、TACACS+ サーバまたは RADIUS サーバでサーバグループに「aaa authentication login default」設定を割り当てると、Telnet/SSH ログインで次のエラーが発生してユーザを認証できません。

「`%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond`」

考えられる原因

サーバにアクセスするための正しい VRF で AAA グループが設定されていません。

解決方法

次の手順を実行してログインをイネーブルにします。

- 「show running-config aaa」コマンドと「show aaa authentication」コマンドを使用して、どの AAA グループが認証に使用されているかを確認します。

- TACACS+ では、「show tacacs-server groups」コマンドと「show running-config tacacs+」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- RADIUS+ では、「show radius-server groups」コマンドと「show running-config radius」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- VRF の関連付けを修正し、「test aaa group <name> <username> <password>」コマンドを使用して VRF 設定をテストします。
- 「test aaa」コマンドを実行すると「user has failed authentication」というエラーが返る場合、サーバはアクセス可能ですが、このユーザアカウントのクレデンシャルが正しくありません。サーバ上のユーザ設定が正しいかどうかを確認します。

考えられる原因

ネットワーク上で AAA サーバがアクセス不能になっています。

解決方法

VRF の関連付けとユーザ アカウントのクレデンシャルを修正しても問題が解決しない場合は、次の手順を実行します。

- 「test aaa」コマンドを実行すると「error authenticating to server」というエラーが返る場合は、設定上でサーバへのルートが欠落している可能性があります。AAA サーバをデフォルトの VRF に関連付けている場合は、「ping <server>」コマンドを使用します。AAA サーバを VRF 管理に関連付けている場合は、「ping <server> vrf management」コマンドを使用します。
- メッセージ「No route to host」が表示される場合は、サーバへのスタティック ルートが適切に設定されていません。該当の VRF コンテキストで IP ルートを設定し直します。
- 再度、「ping <server>」コマンドを入力します。このコマンドを正常に実行できた場合は、「test aaa group <name> <username> <password>」コマンドを使用します。
- 「ping <server>」コマンドを正常に実行できない場合は、ネットワークの接続を確認します。たとえば、「show ip arp [vrf management]」コマンドでネクストホップ ルータの ARP エントリが表示されるかどうか、Nexus 5000 の ARP エントリがネクストホップ ルータの ARP テーブルに存在するかどうかなどを確認します。

Wireshark でパケットの内容をデコードできない

AAA パケットはネットワークからキャプチャできますが、そのパケットの内容を Wireshark でデコードできません。

考えられる原因

ホスト キーがイネーブルとなっているときは、AAA パケットが暗号化されています。

解決方法

次の手順を実行してパケットの内容をデコードします。

- 「no tacacs-server」コマンドを使用して TACACS サーバの設定を削除します。
- どのキーも指定せずに TACACS サーバを再設定します。
- ACS の [Network Configuration] ページで、ホスト キーを削除して、Nexus 5000 向けに AAA クライアントを再設定します。
- もう一度傍受を実行します。キャプチャしたパケットは暗号化されていないので、Wireshark でデータの内容を正しくデコードできます。

- パケットをキャプチャした後、セキュリティを損なわないように、管理者がホスト キーの設定を元に戻す必要があります。

ユーザがログインするとロールの割り当てに失敗する

ユーザがログインすると、ロールの割り当てに失敗します（Nexus 5000 自身の AAA から見た場合）。

考えられる原因

ACS または TACACS+/RADIUS のシスコ属性値（av）ペアが正しく設定されていると仮定すると、ユーザログインに対する内部またはローカルの VRF 割り当てが正しく機能していないことが問題であると考えられます。

解決方法

ロールの割り当てに対して次の手順を実行します。

- 「show running-config aaa」コマンドと「show aaa authentication」コマンドを使用して、どの AAA グループが認証に使用されているかを確認します。
- TACACS+ では、「show tacacs-server groups」コマンドと「show running-config tacacs+」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- RADIUS+ では、「show radius-server groups」コマンドと「show running-config radius」コマンドを使用して、その AAA グループと VRF との関連付けを確認します。
- 上記のコマンドで関連付けが正しいことがわかった場合は、「debug tacacs+ all」コマンドを使用してトレースをイネーブルにします。
- このユーザでもう一度ログインし、デバッグ トレースを収集します。
- このトレースには、詳しい調査に使用できる情報が記録されています（以下の例を参照）。

  例：

  ```
  tacacs: process_aaa_tplus_request: Group t1 found. corresponding vrf is management
  ```

- 「no debug tacacs+ all」コマンドを使用して、TACACS+ でのデバッグ トレースをオフにします。

TACACS+ アカウンティングを有効にすると、ACS サーバ上にコマンド アカウンティングのログが存在しない

TACACS+ アカウンティングを有効にすると、ACS サーバ上にコマンド アカウンティングのログが見つかりません。

考えられる原因

ACS サーバの設定が間違っているか、不完全です。

解決方法

次の手順を実行します。

- ネットワーク設定の ACS の GUI で、任意のクライアントの AAA クライアント設定に移動します。[Log Update/Watchdog Packets from this AAA Client] チェックボックスをオンにします。[Submit + Apply] ボタンをクリックします。

- 次のメニュー パスで CMD アカウンティングを確認します。

  [Reports and Activity] > [TACACS+ Administration]

  「Tacacs+Administration <active|DATE>.csv」ファイルを開き、各行の「cmd」とタイムスタンプを確認します。

RADIUS で PAP 認証が機能しない

TACACS+ では PAP 認証が機能しますが、RADIUS では機能しません。

考えられる原因

NXOS では、リリース 4.2（1）より TACACS+ でのみ ASCII（PAP）認証をサポートするようになりました。

解決方法

NXOS では、ASCII 認証は PAP 認証と同等です。デフォルトでは、TACACS+ と RADIUS はいずれも CHAP を使用します。「aaa authentication login ascii-authentication」コマンドを使用すると、PAP 認証に切り替えることができます。

ユーザが RADIUS と同時に TACACS+ も設定しようとすると、次の例にあるような Syslog メッセージがログインの際に表示されます。

例：

```
2010 May 19 16:12:19 mars %$ VDC-1 %$ %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII
authentication not supported
2010 May 19 16:12:19 mars %$ VDC-1 %$ %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication
failed for user oregon-regress from 10.193.128.5 - login[5698]
```

認証のフォールバック メカニズムが動作していないように見える

NXOS が認証でサポートしているフォールバック メカニズムでは、どの AAA リモート RADIUS サーバにも、またどの AAA リモート TACACS+ サーバにもアクセスできない場合は、ログインの際にローカルで SSH/Telnet ユーザを認証しようとします。しかし、Nexus 5000 へのログインがローカル認証でも失敗します。

考えられる原因

ユーザがログインで使用しているユーザ アカウントが、ローカルのユーザ データベースに存在していません。

解決方法

次の手順を実行して、認証のフォールバック メカニズムを確認します。

- 基本的な手順として、設定で「aaa authentication login error-enable」を指定する必要があります。これを設定で指定すると、フォールバック メカニズムが正しく機能しているかどうかをログイン セッションで確認できます。「Remote AAA servers unreachable; local authentication done」や「Remote AAA servers unreachable; local authentication failed」というメッセージが表示される場合は、フォールバック メカニズムが正しく機能しています。
- AAA サーバにアクセスできない場合は、ローカル認証のためのユーザ クレデンシャルがローカルのユーザ データベースに存在するかどうかを確認します。「show user-account」コマンドを使用してクレデンシャルを表示します。

（注）「show user-account」コマンドでは、REMOTE 認証によってどのユーザ アカウントが作成されているかを確認できます。REMOTE 認証で作成したユーザ アカウントはローカル（フォールバック）ログインで使用できません。

- リモート AAA サーバにアクセスできるようになるまで、「username <username> password <password> role <role name>」コマンドを使用してローカルのユーザ アカウントを作成します。

CHAPTER 7

システム管理上の問題のトラブルシューティング

Cisco Nexus 5000 シリーズ スイッチのシステム管理機能を使用してネットワークをモニタし、管理することで、デバイスの効率的な使用、ロールベースのアクセス制御、SNMP 通信、診断、ロギングなどを実現できます。

この章では、システム管理と Cisco Nexus 5000 シリーズ スイッチで発生する可能性のある問題を特定して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

SNMP

SNMP のメモリ使用量が連続的に増加する

SNMP のメモリ使用量が連続的に増加していることが「show proc mem | inc snmp」コマンドで示されます。

考えられる原因

複数のさまざまなモニタ ステーションで SNMP 要求を処理していると、SNMP のメモリ使用量が増加します。普通は時間の経過とともにメモリ使用量は一定の範囲に落ち着きます。メモリ使用量が安定せずに増加し続ける場合は、メモリ リークを発生している SNMP 要求が存在します。

解決方法

「show system internal snmp mem-stats detail」コマンドの実行結果を確認します。

次のモニタ ステーションで SNMP 要求を処理しているときに、サンプル スナップショットを取得します。

- 「show clock」
- 「show system internal mem-stats detail」
- 「show tech snmp」

SNMP が応答しない

SNMP 要求に対する応答がないか、応答が遅延します。

考えられる原因

GET、GETNEXT、WALK などの SNMP 操作でスイッチの CPU 使用率が高くなると、応答が極端に遅くなり、場合によってはタイムアウトになって応答が得られません。

解決方法

SNMP が応答しない場合は、次のコマンドで CPU 使用率を確認します。

- 「show proc cpu history」
- 「show proc cpu sort」

  このコマンドの実行結果から、Nexus 5000 のコンポーネントのうち、CPU のリソースを大量に消費しているものはどれであるかがわかります。

SNMP が応答せず、SNMP がタイムアウトしたことが「show snmp」で報告される

SNMP が応答せず、SNMP がタイムアウトしたことが「show snmp」コマンドで報告されます。

考えられる原因

SNMP プロセスは終了していますが、クラッシュしていない可能性があります。

解決方法

「show system internal sysmgr service name snmpd」コマンドを実行して、ステートが「SRV_STATE_HANDSHAKED」であることが示される必要があります。

例：

```
Service "snmpd" ("snmpd", 74):
UUID = 0x1A, PID = 4131, SAP = 28
State: SRV_STATE_HANDSHAKED (entered at time Mon Jun 14 17:12:15 2010).
Restart count: 1
Time of last restart: Mon Jun 14 17:12:14 2010.
The service never crashed since the last reboot.
Tag = N/A
Plugin ID: 0
```

SNMP の SET 操作を実行できない

SNMP の SET 操作を実行しようとすると、次のエラーが表示されます。

```
bash-2.05b$ snmpset -v2c -c private 10.78.25.211 .1.3.6.1.4.1.9.9.305.1.1.6.0 i 1
Error in packet.
Reason: notWritable
```

考えられる原因

SNMP コミュニティに書き込み権限がありません。

解決方法

「show snmp community」コマンドの実行結果で、書き込み権限がイネーブルであることを確認します。

例：

```
Community            Group / Access      context    acl_filter

private               network-operator
public                network-admin

Only "network-admin" has write permissions.
                    snmpset -v2c -c public 10.78.25.211 .1.3.6.1.4.1.9.9.305.1.1.6.0 i 1
                   enterprises.9.9.305.1.1.6.0 =
```

BRIDGE-MIB で実行する SNMP

BRIDGE-MIB で実行する SNMP の GET 操作で正しい値が返されず、エラーになります。

考えられる原因

BRIDGE-MIB がサポートされていない可能性があります。

解決方法

該当のリリース ノートを調べ、4.2（1）以降のリリースで BRIDGE-MIB がサポートされていることを確認します。

ロギング

システムが応答しない

システムのパフォーマンスが著しく低いか、応答がありません。

考えられる原因

利用率が異常に高いシステム リソースがあることが考えられます。たとえば、ロギング レベルが正しくないと大量のメッセージが生成され、システム リソースを圧迫することがあります。

解決方法

シャーシに対するロギング レベルを確認します。6 や 7 などのロギング レベルを設定するとメッセージが大量に生成されるので、パフォーマンスに影響することがあります。次のコマンドを使用して、現在のリソース使用量を表示します。

- 「sho proc cpu | inc syslogd」
- 「sho proc cpu」
- 「show run | inc logging」
- 「show system resource」

DUT からのメッセージを Syslog サーバで受信できない

Syslog サーバは設定済みですが、宛先の Syslog サーバでは DUT からのメッセージを受信していません。

考えられる原因

Syslog サーバがアクセス不能になっているか、ロギング レベルが不適切であることが考えられます。

解決方法

- VRF 管理から宛先の Syslog サーバがアクセス可能であるかどうかを確認します。「ping <dest-ip> vrf management」コマンドを使用して、サーバに ping を送信します。
- DUT の Syslog 設定に use-vrf management があることを確認します。

  例：

  ```
  logging server 10.193.12.1 5 use-vrf management
  ```

- ロギング メッセージを送信するために適切なロギング レベルがイネーブルになっていることを確認します。「show logging info」コマンドを使用します。ロギング レベルが不適切な場合は、「logging level <feature> <log-level>」コマンドを使用して適切なレベルを設定します。

トラップ

トラップを受信できない

トラップの結果が受信されません。

考えられる原因

トラップがイネーブルになっていないか、SNMP ホストがアクセス不能になっている可能性があります。

次の原因が考えられます。

- トラップがイネーブルになっていない。
- SNMP ホストがアクセス不能になっている。
- ファイアウォールでアクセスがブロックされている。
- アクセスリストで UDP ポート 162 がブロックされている。

解決方法

次のコマンドを使用して、適切な VRF が SNMP ホストに設定されているかどうか、トラップがイネーブルになっているかどうかを確認します。

- 「snmp-server enable traps <trapname>」
- 「snmp-server host x.x.x.x use-vrf <vrf-name>」
  x.x.x.x は、トラップを受信するデバイスの IP アドレスです。

INDEX

ほ

ま

れ

ろ