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

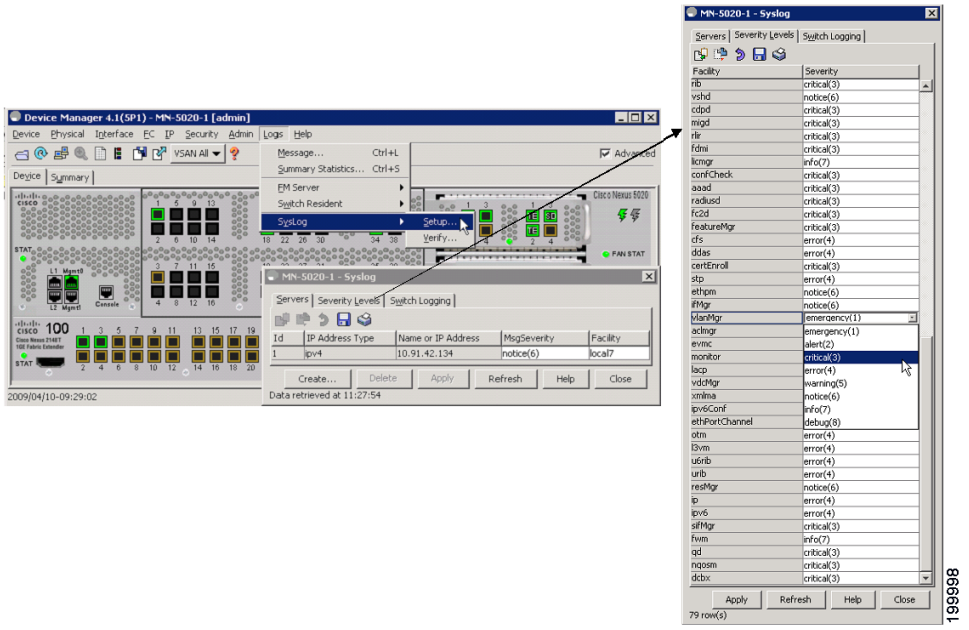
CLI または Device Manager を通じてロギングを使用できます。次に、**logging** コマンドと Device Manager によって重大度情報を表示する例を示します。

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）。

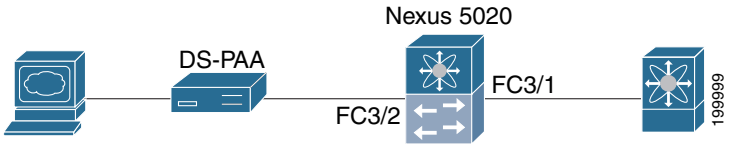
設定に関する制限：VLAN またはポートチャネルを出力送信元として設定できない

- 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。