CHAPTER 1

トラブルシューティングの概要

この章では、Cisco Nexus 1000V の設定または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。

この章は、次の内容で構成されています。

トラブルシューティング プロセスの概要

ネットワークに関するトラブルシューティングの一般的な手順は、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。

ベスト プラクティスの概要

ベスト プラクティスとは、ネットワーク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。次の一般的なベスト プラクティスは、ほとんどのネットワークに推奨されます。

- すべてのネットワーク デバイスで、Cisco Nexus 1000V リリースの一貫性を保持します。
- Cisco Nexus 1000V 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。「現象の概要」（P.1-4）を参照してください。
- 変更を実装したら、新しい設定変更を確認してトラブルシューティングを実施します。

トラブルシューティングの基本

ここでは、Cisco Nexus 1000V または接続されているデバイスに関する問題のトラブルシューティングを実施する際に寄せられる質問を紹介します。これらの質問への回答に従って、問題の範囲を識別し、一連の処置を計画します。

ここでは、次の内容について説明します。

トラブルシューティングのガイドライン

次の質問に回答することにより、従う必要がある手順および詳細に調査する必要があるコンポーネントを決定できます。

次の質問に回答することにより、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（新規のホスト、スイッチ、または Virtual Local Area Network（VLAN; バーチャル LAN）である可能性があります）。
- これまでにホストがネットワークを認識していた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。

ネットワークの問題を検出するには、次の一般的なネットワーク トラブルシューティング手順に従います。

ステップ 1　システムにおける問題に関する情報を収集します。「情報の収集」（P.1-3）を参照してください。

ステップ 2　レイヤ 2 接続を確認します。「レイヤ 2 接続の確認」（P.1-3）を参照してください。

ステップ 3　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 4　エンドツーエンド接続を確認します。「レイヤ 3 接続の確認」（P.1-4）を参照してください。

情報の収集

ここでは、ネットワークにおける問題のトラブルシューティングで一般的に使用されるツールについて説明します。これらのツールは、特定の問題のトラブルシューティングに使用する可能性があるツールの一部です。

各章には、その章に関連する現象および考えられる問題に個別に対応するツールおよびコマンドが掲載されています。

問題領域を絞り込むためには、ネットワークの正確なトポロジを把握している必要もあります。

次のコマンドを実行して、出力を調べます。

- **show module**
- **show version**
- **show running-config**
- **show logging log**
- **show interfaces brief**
- **show vlan**
- **show accounting log**
- **show tech support svs**

（注）　**internal** キーワードを指定してコマンドを実行するには、ネットワーク管理者ロールを使用してログインする必要があります。

ポートの確認

ポートを確認するには、次の質問に回答します。

- 正しいメディア（銅線、光）およびファイバ タイプを使用していることを確認します。
- メディアが故障または破損していないことを確認します。
- 仮想イーサネットポートを検査していることを確認します。検査している場合は、**show interface brief** コマンドを使用します。ステータスが up である必要があります。
- 物理イーサネットポートを検査していることを確認します。検査している場合は、サーバを調べるか、アップストリーム スイッチを調べる必要があります。
- Virtual Supervisor Module（VSM; 仮想スーパーバイザ モジュール）Virtual Machine（VM; 仮想マシン）のネットワーク アダプタに正しいポート グループが割り当てられているかどうか、およびそれらがすべて vSphere Client に接続されているかどうかを調べます。

レイヤ 2 接続の確認

レイヤ 2 接続を確認するには、次の質問に回答します。

- 必要なインターフェイスが同一の VLAN 内に存在することを確認します。
- 速度、デュプレックス、トランクの各モードについて、ポート チャネル内のすべてのポートの設定が同じであることを確認します。

show vlan brief コマンドを使用します。ステータスが up である必要があります。

ポートのプロファイル設定を調べるには、**show port-profile** コマンドを使用します。

仮想イーサネット ポートまたは物理イーサネット ポートのステータスを調べるには、**show interface-brief** コマンドを使用します。

レイヤ 3 接続の確認

レイヤ 3 接続を確認するには、次の質問に回答します。

- ラスト リゾート ゲートウェイを設定したことを確認します。
- IP アクセス リスト、フィルタ、ルート マップによって、ルート アップデートがブロックされていないことを確認します。

接続を確認するには、**ping** コマンドまたは **trace** コマンドを使用します。詳細については、次のセクションを参照してください。

- 「ping」（P.2-2）
- 「traceroute」（P.2-2）

現象の概要

現象に基づいたトラブルシューティング手法では、問題を診断して解決するための複数の方法が提供されます。このマニュアルは、解決方法へのリンクを含む複数のエントリ ポイントを使用することにより、さまざまな指標によって認識される同一の問題を持つ可能性があるユーザに役立つように設計されています。必要な情報に効率的にアクセスするためのエントリ ポイントとして、この PDF 形式のマニュアルを検索する、インデックスを使用する、または各章に記載されている現象と診断の説明に従います。

最小限のネットワークの中断で問題を解決するには、記載されている観察可能なネットワークの現象に基づいて、ソフトウェアの設定の問題や操作不可能なハードウェア コンポーネントを診断して修正できることが重要です。次に、問題と対処方法を示します。

- 主要な Cisco Nexus 1000V トラブルシューティング ツールを特定します。
- CLI で Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）または Ethanalyzer を使用し、プロトコル トレースを取得して分析します。
- 物理ポートの問題を識別または除外します。
- スイッチ モジュールの問題を識別または除外します。
- レイヤ 2 の問題を診断および修正します。
- レイヤ 3 の問題を診断および修正します。
- Technical Assistance Center（TAC）で使用されるコア ダンプおよびその他の診断データを取得します。
- スイッチをアップグレードの障害から復旧します。

システム メッセージ

システム ソフトウェアは、動作中に、Syslog（システム）メッセージをコンソール（およびオプションとして別のシステム上にあるログ収集サーバ）に送信します。ただし、すべてのメッセージがシステムの問題を表すとは限りません。一部のメッセージは単に情報を示すだけですが、リンク、内蔵ハードウェア、またはシステム ソフトウェアに関する問題の診断に役立つメッセージもあります。

ここでは、次の項目について説明します。

システム メッセージ テキスト

メッセージ テキストは、状態を説明するテキスト ストリングです。メッセージのこの部分には、イベントについての詳細な情報が含まれている場合があります。含まれる情報は、端末ポート番号、ネットワーク アドレス、またはシステム メモリのアドレス空間内での位置に対応するアドレスです。この可変フィールドの情報はメッセージごとに異なるので、ここでは角カッコで囲んだ短い文字列で示します。たとえば 10 進数は [dec] で表します。

```
2009 Apr 29 12:35:51 n1000v %KERN-1-SYSTEM_MSG: stun_set_domain_id : Setting domain ID
(1024) - kernel
```

この文字列を使用して、『*Cisco NX-OS System Messages Reference System Messages Reference*』で一致するシステム メッセージを検索してください。

各システム メッセージのあとには、説明と推奨処置が記載されています。この処置は「No action required」のような簡単なものであることもありますが、次の例のように、修正方法に関するものやテクニカル サポートへの連絡を推奨するものもあります。

エラー メッセージ　`2009 Apr 29 14:57:23 n1000v %MODULE-5-MOD_OK: Module 3 is online (serial: )`

説明　VEM モジュールがスロット 3 に正常に挿入されました。

推奨処置　なし。これは、通知のメッセージです。スロット 3 にあるモジュールを確認するには「show module」を使用してください。

Syslog サーバの実装

Syslog ファシリティを使用して、Cisco Nexus 1000V デバイスからメッセージ ログのコピーをホストに送信すると、ログ用により多くの永続的ストレージを確保できます。この方法は、長期間にわたってログを調べる必要がある場合や、Cisco Nexus 1000V デバイスにアクセスできない場合に役立つ可能性があります。

次に、Solaris プラットフォーム上で Syslog ファシリティを使用するように Cisco Nexus 1000V デバイスを設定する例を示します。ここでは Solaris ホストを使用しますが、すべての UNIX および Linux システムにおける Syslog の設定は非常によく似ています。

Syslog では、ファシリティの概念を使用して、Syslog サーバ上での処理方法とメッセージの重大度が決定されます。このため、Syslog サーバでは、異なるメッセージの重大度を異なる方法で処理できます。たとえば、メッセージを別々のファイルに記録することや、特定のユーザに電子メールで送信することもできます。重大度を指定すると、そのレベル以上の重大度（より低い数値）のすべてのメッセージに対して処置が行われます。

（注） Cisco Nexus 1000V メッセージは、他社の Syslog メッセージと競合しないように、標準 Syslog ファイルとは別のファイルに記録される必要があります。/ ファイル システムがログ メッセージでいっぱいになることを防ぐため、ログファイルは / ファイル システムに配置しないでください。
Syslog クライアント：switch1
Syslog サーバ：172.22.36.211（Solaris）
Syslog ファシリティ：local1
Syslog の重大度：通知（レベル 5、デフォルト）
Cisco Nexus 1000V メッセージを記録するログ ファイル：/var/adm/nxos_logs

Syslog サーバを設定するには、次の手順に従います。

ステップ 1　Cisco Nexus 1000V を設定します。

```
n1000v# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
n1000v(config)# logging server 192.0.2.1 6 facility local1
```

設定を表示するには、次のように入力します。

```
n1000v# show logging server
Logging server: enabled
{192.0.2.1}
     server severity: notifications
     server facility: local1
```

ステップ 2　Syslog サーバを設定します。

a. local1 のメッセージを処理するように、/etc/syslog.conf を変更します。Solaris の場合は、facility.severity と処置（/var/adm/nxos_logs）の間に少なくとも 1 つのタブが必要です。

```
#Below is for the NX-OS logging
local1.notice /var/adm/nxos_logs
```

b. ログ ファイルを作成します。

```
#touch /var/adm/nxos_logs
```

c. Syslog を再起動します。

```
# /etc/init.d/syslog stop
# /etc/init.d/syslog start
syslog service starting.
```

d. Syslog が再起動されたことを確認します。

```
# ps -ef |grep syslogd
     root 23508 1 0 11:01:41 ? 0:00 /usr/sbin/syslogd
```

ステップ 3　Cisco Nexus 1000V でイベントを作成して、Syslog サーバをテストします。この場合、ポート e1/2 はバウンスされ、Syslog サーバ上で次のように表示されます。スイッチの IP アドレスは角カッコで囲まれています。

```
# tail -f /var/adm/nxos_logs
Sep 17 11:07:41 [172.22.36.142.2.2] : 2004 Sep 17 11:17:29 pacific:
%PORT-5-IF_DOWN_INITIALIZING: %$VLAN 1%$ Interface e 1/2 is down (Initializing)
```

```
Sep 17 11:07:49 [172.22.36.142.2.2] : 2004 Sep 17 11:17:36 pacific: %PORT-5-IF_UP:
%$VLAN 1%$ Interface e 1/2 is up in mode access
Sep 17 11:07:51 [172.22.36.142.2.2] : 2004 Sep 17 11:17:39 pacific:
%VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
(dhcp-171-71-49-125.cisco.com)
```

ログによるトラブルシューティング

Cisco Nexus 1000V では、スイッチ上でさまざまなタイプのシステム メッセージを生成して、Syslog サーバに送信します。これらのメッセージを確認することにより、現在発生している問題の原因となった可能性のあるイベントを判別できます。

ログの表示

Cisco Nexus 1000V のログにアクセスして表示するには、次のコマンドを使用します。

```
n1000v# show logging ?

console        Show console logging configuration
info           Show logging configuration
internal       syslog syslog internal information
last           Show last few lines of logfile
level          Show facility logging configuration
logfile        Show contents of logfile
loopback       Show logging loopback configuration
module         Show module logging configuration
monitor        Show monitor logging configuration
nvram          Show NVRAM log
pending        server address pending configuration
pending-diff   server address pending configuration diff
server         Show server logging configuration
session        Show logging session status
status         Show logging status
timestamp      Show logging timestamp configuration
|              Pipe command output to filter
```

例 1-1 に、**show logging** コマンドの出力例を示します。

例 1-1　　show logging コマンド

```
n1000v# show logging server
Logging server: enabled
{192.0.1.1}
server severity: critical
server facility: user
```

シスコのサポート コミュニティ

詳細については、次のいずれかのサポート コミュニティにアクセスしてください。

- Cisco Support Community for Server Networking
- Cisco Communities : Nexus 1000V

シスコまたは VMware のカスタマー サポートへの連絡

このマニュアルのトラブルシューティング情報を使用しても問題を解決できない場合には、カスタマーサービス担当者に連絡して、支援および詳細な指示を受けてください。担当者ができる限りすばやいサポートを行えるように、連絡する前に次の情報を用意してください。

- 実行している Nexus 1000V ソフトウェアのバージョン
- 実行している ESX Server および vCenter Server ソフトウェアのバージョン
- 連絡先電話番号
- 問題点の要約
- 問題を特定し、解決するためにすでに実施した手順の簡単な説明

Cisco Nexus 1000V およびサポート契約をシスコから購入された場合は、シスコに Nexus 1000V のサポートをご依頼ください。シスコは、L1、L2、および L3 のサポートを提供します。

Cisco Nexus 1000V および SNS を VMware から購入された場合は、VMware に Nexus 1000V のサポートをご依頼ください。VMware は、L1 および L2 のサポートを提供します。シスコは、L3 のサポートを提供します。

これらの情報を収集してから、「関連資料」（P.xv）を参照してください。

テクニカル サポートへ問い合わせる前に実施する手順の詳細については、「テクニカル サポートへ問い合わせるための情報の収集」（P.24-1）を参照してください。