CHAPTER 7

# STP のトラブルシューティング

この章では、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）の実装時に発生する可能性がある問題を識別して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

# STP のトラブルシューティングについて

STP は、レイヤ 2 レベルで、ループフリー（ループが発生しない）ネットワークを実現します。レイヤ 2 LAN ポートは、一定の間隔で STP フレームを送受信します。ネットワーク デバイスは、これらのフレームを転送せずに、フレームを使用してループフリー パスを構築します。詳細については、『*Cisco NX-OS Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。

STP を設定する際は、次のガイドラインに従ってください。

- Multiple STP（MST）とともにプライベート VLAN を使用する場合は、すべてのセカンダリ VLAN がプライマリ VLAN と同じ MST インスタンスに属していることを確認します。
- ネットワーク上のすべての VLAN のスパニング ツリーをディセーブルにせずに、802.1Q トランクのネイティブ VLAN のスパニング ツリーをディセーブルにすると、スパニング ツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN 上のスパニング ツリーは、イネーブルのままにしておく必要があります。そうできない場合は、ネットワークのすべての VLAN のスパニング ツリーをディセーブルにする必要があります。スパニング ツリーをディセーブルにする前に、ネットワークで物理ループが発生しないことを確認してください。
- 802.1Q トランクを使用して 2 台のシスコ製スイッチを接続する場合、トランク上で許容されている VLAN ごとにスパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしで予約 IEEE 802.1D スパニング ツリー マルチキャスト MAC（メディア アクセス制御）アドレス（01-80-C2-00-00-00）に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きで予約 Cisco Shared Spanning Tree（SSTP）マルチキャスト MAC アドレス（01-00-0c-cc-cc-cd）に送信されます。
- STP では、ポートチャネル バンドルはシングル ポートと見なされます。この場合のポート コストは、そのチャネルに割り当てられているすべての設定済みポート コストの合計です。
- セカンダリ VLAN がプライマリ VLAN に関連付けられている場合、ブリッジ プライオリティなどの 0 プライマリ VLAN の STP パラメータは、セカンダリ VLAN に伝播されます。ただし、他のデバイスに STP パラメータを伝播する必要はありません。VLAN が同一の転送データベースを適切に共有できるように、プライマリ、独立、およびコミュニティ VLAN のスパニング ツリー トポロジが厳密に一致していることを確認するには、STP 設定を手動で検証する必要があります。
- 通常のトランク ポート：
  - プライベート VLAN 内の各 VLAN には、個別に STP インスタンスが存在します。
  - プライマリ VLAN およびすべてのセカンダリ VLAN の STP パラメータは、一致する必要があります。
  - プライマリ VLAN および関連するすべてのセカンダリ VLAN は、同一の MST インスタンスに設定する必要があります。
  - トラフィックが多い状況での衝突を防止するために、リンクの両側のデュプレックス設定を full に設定する必要があります。
- 非トランク ポート：
  - STP は、プライベート VLAN ホスト ポートのプライマリ VLAN のみを認識します。STP は、ホスト ポートのセカンダリ VLAN 上では実行されません。
- プライベート VLAN 上の Rapid PVST+：
  - トランク ポートでは、プライマリおよびセカンダリ プライベート VLAN は 2 つの異なる論理ポートであり、同一の STP トポロジを持つ必要があります。
  - アクセス ポートでは、STP はプライマリ VLAN のみを認識します。

**（注）** 一部のケースでは、エラー　メッセージが表示されずに設定が許可されても、コマンドは無効である場合があります。

# トラブルシューティングの初期チェックリスト

STP の問題のトラブルシューティングでは、個々のデバイスおよびネットワーク全体の設定と接続に関する情報を収集する必要があります。STP に関する問題のトラブルシューティングを開始する際は、まず、次の事項について確認します。

| チェックリスト | 確認済み |
|---|---|
| LAN 内のすべてのポートに設定されているスパニング ツリーのタイプを確認します。 | ❑ |
| ネットワーク トポロジ（相互接続されたすべてのポートとスイッチを含む）を確認します。 | ❑ |
| **show spanning-tree summary totals** コマンドを使用して、Active ステートの論理インターフェイスの合計数が、許可されている最大数よりも少ないことを確認します。これらの制限の詳細については、『*Cisco NX-OS Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。 | ❑ |
| プライマリおよびセカンダリ ルート ブリッジ、設定されているシスコの拡張機能を確認します。 | ❑ |
| ポートがブロックされている場合、隣接デバイスとデュプレックス設定が同じであることを確認します。 | ❑ |
| トランク設定が、リンクの両側で一致していることを確認します。 | ❑ |

次のコマンドを使用して、STP 設定および動作の詳細を表示します。

- **show running-config spanning-tree**
- **show spanning-tree summary**
- **show spanning-tree detail**
- **show spanning-tree mst**
- **show spanning-tree mst configuration**
- **show spanning-tree interface** *interface-type slot/port* [**detail**]
- **show tech-support stp**
- **show spanning-tree vlan**

**show spanning-tree blockedports** コマンドを使用して、STP にブロックされているポートを表示します。

**show mac address-table dynamic vlan** コマンドを使用して、各ノードで学習やエージングが発生しているかを判別します。

# STP データ ループのトラブルシューティング

データ ループは、STP ネットワークでは一般的な問題です。データ ループが発生すると、次のような症状が現れます。

- リンクの使用率が高くなる（最大 100%）
- CPU の使用率、およびバックプレーンのトラフィックの使用率が高くなる
- MAC アドレスの再学習とフラッピングが絶えず発生する
- インターフェイス上で多くの出力が廃棄される

STP ループのトラブルシューティングを行う手順は、次のとおりです。

**ステップ 1**　リンクの使用率が高いインターフェイスを探し、ループに関連しているポートを特定します。

```
switch# show interface ethernet 2/1 | include rate
  5 minute input rate 9976523 bytes/sec, 25912 packets/sec
  5 minute output rate 985644 bytes/sec, 32456 packets/sec
```

**ステップ 2**　影響を受けているポートをシャットダウンするか、接続解除します。

```
switch(config)# interface ethernet 2/1
switch(config-if)# shutdown
```

**ステップ 3**　ネットワーク トポロジ図を使用して、冗長パス上のすべてのスイッチを見つけます。

**ステップ 4**　このスイッチが、影響を受けていない他のスイッチと同じ STP ルート ブリッジを表示することを確認します。

```
switch# show spanning-tree vlan 9

VLAN0009
  Spanning tree enabled protocol rstp
  Root ID     Priority    32777
              Address     0018.bad7.db15
              Cost        4
...
```

**ステップ 5**　ルート ポートが、ルート ブリッジへのコストが最小となるポートとして正しく識別されていることを確認します。

```
switch# show spanning-tree vlan 9

VLAN0009
  Spanning tree enabled protocol rstp
  Root ID     Priority    32777
              Address     0018.bad7.db15
              Cost        4
              Port        385 (Ethernet3/1)
              Hello Time  2  sec  Max Age 20 sec  Forward Delay 15 sec
```

**ステップ 6**　ルート ポートおよび代替ポートで、BPDU が定期的に受信されていることを確認します。

```
switch# show spanning-tree interface ethernet 3/1 detail

 Port 385 (Ethernet3/1) of VLAN0001 is root forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.385
   Designated root has priority 32769, address 0018.bad7.db15
   Designated bridge has priority 32769, address 0018.bad7.db15
   Designated port id is 128.385, designated path cost 0
   Timers: message age 16, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port type is network by default
   Link type is point-to-point by default
   BPDU: sent 1265, received 1269
```

**ステップ 7**　受信 BPDU カウンタが増加していない場合、内部パケット マネージャが BPDU を受信しているかどうかをチェックします。

```
switch# show system internal pktmgr interface ethernet 3/1
Ethernet3/1, ordinal: 36
  SUP-traffic statistics: (sent/received)
    Packets: 120210 / 15812
    Bytes: 8166401 / 1083056
    Instant packet rate: 5 pps / 5 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
      Tx: Unicast 0, Multicast 120210
          Broadcast 0
      Rx: Unicast 0, Multicast 15812
          Broadcast 0

switch# show system internal pktmgr client 303
Client uuid: 303, 2 filters
  Filter 0: EthType 0x4242,  Dmac 0180.c200.0000
  Filter 0: EthType 0x010b, Snap 267, Dmac 0100.0ccc.cccd

  Options: TO 0, Flags 0x1, AppId 0, Epid 0
  Ctrl SAP: 171, Data SAP 177 (1)
  Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0
```

**ステップ 8**　パケット マネージャが BPDU を受信していない場合、ハードウェア パケット統計情報（エラー ドロップ）カウンタをチェックします。

```
switch# show interface counters errors

--------------------------------------------------------------------------------
Port       Align-Err     FCS-Err    Xmit-Err     Rcv-Err   UnderSize OutDiscards
--------------------------------------------------------------------------------
mgmt0             --          --          --          --          --          --
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
```

**ステップ 9**　指定ポートが定期的に BPDU を送信していることをチェックします。

```
switch# show spanning-tree interface ethernet 3/1 detail

 Port 385 (Ethernet3/1) of VLAN0001 is root forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.385
   Designated root has priority 32769, address 0018.bad7.db15
   Designated bridge has priority 32769, address 0018.bad7.db15
   Designated port id is 128.385, designated path cost 0
   Timers: message age 16, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port type is network by default
   Link type is point-to-point by default
   BPDU: sent 1265, received 1269
```

**ステップ 10**　BPDU 送信カウンタが増加している場合、パケット マネージャが BPDU を送信しているかどうかをチェックします。

```
switch# show system internal pktmgr interface ethernet 3/1
Ethernet3/1, ordinal: 36
  SUP-traffic statistics: (sent/received)
    Packets: 120210 / 15812
    Bytes: 8166401 / 1083056
    Instant packet rate: 5 pps / 5 pps
    Average packet rates(1min/5min/15min/EWMA):
    Packet statistics:
     Tx: Unicast 0, Multicast 120210
         Broadcast 0
     Rx: Unicast 0, Multicast 15812
         Broadcast 0

switch# show pktmgr client 303
Client uuid: 303, 2 filters
  Filter 0: EthType 0x4242,  Dmac 0180.c200.0000
  Filter 0: EthType 0x010b, Snap 267, Dmac 0100.0ccc.cccd

  Options: TO 0, Flags 0x1, AppId 0, Epid 0
  Ctrl SAP: 171, Data SAP 177 (1)
  Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0
```

**ステップ 11**　パケット マネージャの BPDU 送信カウンタが増加している場合、ハードウェア パケット統計情報カウンタで、BPDU エラー ドロップの可能性をチェックします。

```
switch# show interface counters errors

--------------------------------------------------------------------------------
Port       Align-Err     FCS-Err    Xmit-Err     Rcv-Err   UnderSize OutDiscards
--------------------------------------------------------------------------------
mgmt0             --          --          --          --          --          --
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
```

# 過度のパケット フラディングのトラブルシューティング

STP トポロジの不安定な変更によって、STP ネットワークで過度のパケット フラッディングが発生することがあります。Rapid STP または Multiple STP（MST）では、ポートの状態が forwarding に変更されたときだけでなく、役割が designated から root に変更された場合にもトポロジの変更が発生します。Rapid STP では、レイヤ 2 転送テーブルが即座にフラッシュされます。802.1D では、エージング タイムが短縮されます。転送テーブルが即座にフラッシュされると、接続はより早く復元されますが、フラッディングは増加します。

安定したトポロジでは、1 度のトポロジの変更によって過度のフラッディングが発生することはありません。トポロジはリンク フラップによって変更されるため、リンク フラップが絶え間なく発生するとトポロジ変更が繰り返され、フラッディングが引き起こされる場合があります。フラッディングにより、ネットワーク パフォーマンスが低下し、インターフェイスのパケット ドロップが発生することがあります。

過度なフラッディングのトラブルシューティングを行う手順は、次のとおりです。

**ステップ 1**　過度なトポロジ変更の発生元を判別します。

```
switch# show spanning-tree vlan 9 detail

 VLAN0009 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 9, address 0018.bad8.27ad
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32777, address 0018.bad7.db15
  Root port is 385 (Ethernet3/1), cost of root path is 4
  Topology change flag not set, detected flag not set
  Number of topology changes 8 last change occurred 1:32:11 ago
          from Ethernet3/1
  Times:  hold 1, topology change 35, notification 2
...
```

**ステップ 2**　トポロジ変更が発生したインターフェイスを判別します。

```
switch# show spanning-tree vlan 9 detail

 VLAN0009 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 9, address 0018.bad8.27ad
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32777, address 0018.bad7.db15
  Root port is 385 (Ethernet3/1), cost of root path is 4
  Topology change flag not set, detected flag not set
  Number of topology changes 8 last change occurred 1:32:11 ago
          from Ethernet3/1
  Times:  hold 1, topology change 35, notification 2
...
```

**ステップ 3**　トポロジ変更を引き起こしていたデバイスを絞り込めるまで、このインターフェイスに接続されているデバイスでステップ 2 を繰り返します。

**ステップ 4**　このデバイスのインターフェイスのリンク フラップをチェックします。

# コンバージェンス時間に関する問題のトラブルシューティング

STP コンバージェンスでは、予想以上に時間がかかる場合や、最終的なネットワーク トポロジが予測とは異なってしまうことがあります。

コンバージェンスに関連する問題のトラブルシューティングを開始するときは、最初に、次の事項について確認します。

- 記録されたネットワーク トポロジ図の誤り
- 設定の誤り — タイマー、直径、シスコの拡張機能（ブリッジ保証、ルート ガード、BPDU ガードなど）の設定に誤りがないことをチェックします。
- コンバージェンス中に、推奨する論理ポート（port-vlan）の制限を越える過大な負荷がスイッチの CPU にかかっている

**（注）** 推奨されるスケーラビリティの制限は、VDC 単位ではなく、システム全体での制限です。

- STP に影響を与える、ソフトウェアの欠陥

# フォワーディング ループからのネットワークの保護

STP によって特定の障害が正しく対処できないという問題に取り組むため、シスコでは多数の機能および拡張機能を開発し、ネットワークをフォワーディング ループから保護しています。

STP のトラブルシューティングは、特定の障害の原因の絞り込みや発見に役立ちますが、ネットワークをフォワーディング ループから保護するには、このような拡張機能を実装することが唯一の手段となります。

ネットワークをフォワーディング ループから保護する手順は、次のとおりです。

**ステップ 1**　すべてのスイッチ間リンクで、シスコ独自の UniDirectional Link Detection（UDLD; 単一方向リンク検出）プロトコルをイネーブルにします。詳細については、『*Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』の UDLD のセクションを参照してください。

**ステップ 2**　すべてのスイッチ間リンクをスパニング ツリー ネットワーク ポート タイプとして設定することで、ブリッジ保証機能をイネーブルにします。

**（注）**　ブリッジ保証機能は、リンクの両側でイネーブルにする必要があります。そのように設定しない場合、Cisco NX-OS はブリッジ保証の不整合のためにポートを blocked 状態に移行させます。

**ステップ 3**　すべてのエンドステーション ポートを、スパニング ツリー エッジ ポート タイプとして設定します。

Topology Change（TC; トポロジ変更）通知およびそのあとに発生するフラッディングは、ネットワークのパフォーマンスに影響を与える可能性があるため、STP エッジ ポートを設定して量を制限する必要があります。このコマンドは、エンド ステーションと接続されているポートでのみ使用してください。それ以外のポートで使用すると、トポロジで偶発的にループが発生したときに、データパケットのループが発生し、デバイスおよびネットワークの動作が中断することがあります。

**ステップ 4**　ポートチャネルの設定の誤りの問題を回避するために、ポート チャネルに対して Link Aggregation Control Protocol（LACP）をイネーブルにします。詳細については、『*Cisco NX-OS Interfaces Configuration Guide, Release 4.0*』の LACP のセクションを参照してください。

スイッチ間リンクの自動ネゴシエーションはディセーブルにしないでください。自動ネゴシエーション メカニズムは、リモートの障害情報を最も早く伝達することができます。リモート側で障害が検出された場合、リンクがパルス受信を続けていても、ローカル側はリンクをダウンさせます。

**注意**　STP タイマーを変更するときは、細心の注意を払ってください。STP タイマーは相互に依存しているため、タイマーの変更がネットワーク全体に影響を与えることがあります。

**ステップ 5**　（任意）**spanning-tree loopguard default** コマンドを使用して、DoS 攻撃（サービス拒絶攻撃）を防止し、ルート ガードによってネットワーク STP 境界を保護します。ルート ガードと BPDU ガードによって、外部の影響から STP を保護できます。

**ステップ 6**　**spanning-tree bpduguard enable** コマンドを使用して BPDU ガードおよび STP エッジ ポートをイネーブルにし、ポートに接続されている不正なネットワーク デバイス（ハブ、スイッチ、ブリッジ ルータなど）による STP への影響を防止します。

ルート ガードにより、STP は外部の影響から保護されています。BPDU ガードをイネーブルにすると、（優良な BPDU だけでなく）すべての BPDU を受信しているポートがシャットダウンされます。

**（注）**　2 つの STP エッジ ポートが直接、またはハブを経由して接続されている場合、短時間のループは、ルート ガードまたは BPDU ガードでは防ぐことはできません。

**ステップ 7**　**vlan** コマンドを使用して独立した VLAN を設定し、管理 VLAN 上でのユーザ トラフィックを防ぎます。管理 VLAN は、ネットワーク全体でなく、1 つのビルディング ブロックに限定します。

**ステップ 8**　**spanning-tree vlan** *vlan-range* **root primary** コマンドを使用して、予測可能な STP ルートを設定します。

**ステップ 9**　**spanning-tree vlan** *vlan-range* **root secondary** コマンドを使用して、予測可能なバックアップ STP ルート配置を設定します。

STP ルートとバックアップ STP ルートを設定することで、コンバージェンスが予測どおりに発生し、常に最適のトポロジが構築されるようにする必要があります。STP の優先順位をデフォルト値のままにしないでください。