STP のトラブルシューティング

STP のトラブルシューティング

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは定期的に 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。レイヤ 2 の詳細については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

STP の初期トラブルシューティングのチェックリスト

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 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。

チェックリスト	Done
デバイスで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。	
すべての相互接続ポートとスイッチを含む、ネットワーク トポロジを確認します。ネットワーク上のすべての冗長パスを特定し、冗長パスはブロック状態であることを確認します。	

チェックリスト	Done
show spanning-tree summary totals コマンドを使用し、 して、アクティブ状態の論理インターフェイスの総数が、最大許容数を下回っていることを確認します。これらの限界値の詳細については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』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 ブリッジと、設定されている Cisco 拡張機能を確認します。	

STP 設定と動作の詳細を表示するには、次のコマンドを使用します。

- **show running-config spanning-tree**
- **show spanning-tree summary**
- **show spanning-tree detail**
- **show spanning-tree bridge**
- **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**

STP によってブロックされているポートを表示するには、**show spanning-tree blockedports** コマンドを使用します。

各ノードで学習またはエージングが発生するかどうかを確認するには、**show mac address-table dynamic vlan** コマンドを使用します。

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 ネットワークでよく見られる問題です。データ ループの症状の一部は次のとおりです。

- 高いリンク使用率、最大 100％
- 高い CPU およびバックプレーン トラフィック使用率
- 一定の MAC アドレスの再学習とフラッピング
- インターフェイスでの過剰な出力ドロップ

l2fm ロギング レベルが 4 以上の場合、スイッチはホスト MAC アドレス フラッピングの発生をログに記録し、STP データ ループの特定に役立ちます。1 秒以内に MAC アドレスの移動が検出され、10 回連続して移動すると、スイッチは MAC アドレスが移動しているポートの 1 つの VLAN で学習を無効にします。学習は 120 秒間無効になり、自動的に再度有効になります。

Syslog は、学習が無効または有効になっている間に生成されます。**logging level l2fm** *log-level* コマンドを使用して、ログ レベルを設定できます。

手順の概要

1. switch# **show interface** *interface-type slot*/*port* **include rate**
2. switch(config)# **interface** *interface-type slot*/*port*
3. switch(config-if)# **shutdown**
4. switch(config-if)# **show spanning-tree vlan** *vlan-id*
5. （任意） switch(config-if)# **show spanning-tree interface** *interface-type slot*/*port* **detail**
6. （任意） switch(config-if)# **show system internal pktmgr interface** *interface-type slot*/*port*
7. （任意） switch(config-if)# **show system internal pktmgr client** *client-id*
8. （任意） switch(config-if)# **show interface counters errors**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	switch# **show interface** *interface-type slot*/*port* **include rate**
	例：
	`switch# show interface ethernet 2/1 include rate`
	`1 minute input rate 19968 bits/sec, 0 packets/sec`
	`1 minute output rate 3952023552 bits/sec, 957312 packets/sec`
		リンク使用率が高いインターフェイスを調べることで、ループに関与するポートを特定します。

ステップ 2	switch(config)# **interface** *interface-type slot*/*port* 例： `switch(config)# interface ethernet 2/1`	インターフェイス タイプと位置を設定します。
ステップ 3	switch(config-if)# **shutdown** 例： `switch(config-if)# shutdown`	影響を受けるポートをシャットダウンまたは切断します。 影響を受けるポートを切断した後、ネットワーク トポロジ図を使用して冗長パス内のすべてのスイッチを特定します。

ステップ 4	switch(config-if)# **show spanning-tree vlan** *vlan-id*
	例：
	`switch(config-if)# show spanning-tree vlan 9`
	`VLAN0009`
	`Spanning tree enabled protocol rstp`
	`Root ID Priority 32777''`
		スイッチが、影響を受けないその他のスイッチと同じ STP ルート ブリッジをリストすることを確認します。

	コマンドまたはアクション	目的
	Address 0018.bad7.db15'' Cost 4 ...	
ステップ 5	（任意） switch(config-if)# **show spanning-tree interface** *interface-type slot/port* **detail** 例： switch(config-if)# 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	ルート ポートおよび代替ポートが BPDU を定期的に受信していることを確認します。
ステップ 6	（任意） switch(config-if)# **show system internal pktmgr interface** *interface-type slot/port* 例： switch(config-if)# 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	内部パケット マネージャが BPDU を受信したかどうかを確認します。
ステップ 7	（任意） switch(config-if)# **show system internal pktmgr client** *client-id* 例： switch(config-if)# 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	クライアントが BPDU を受信したかどうかを確認します。

	コマンドまたはアクション	目的
	Ctrl SAP: 171, Data SAP 177 (1) Rx: 28356632, Drop: 0, Tx: 35498365, Drop: 0	

ステップ 8	（任意） switch(config-if)# **show interface counters errors**
	例：
	`switch(config-if)# 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`
		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。

例

次に、指定ポートが定期的に BPDU を送信している例を示します。

```
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
```

次に、BPDU がパケット マネージャによって送信されているかどうかを確認する例を示します。

```
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, M'' ulticast 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
```

次に、ハードウェアパケット統計カウンタでBPDUエラードロップの可能性をチェックする例を示します。

```
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
```

過剰なパケットフラッディングのトラブルシューティング

STP トポロジが不安定になると、STP ネットワークで過剰なパケットフラッディングが発生する可能性があります。Rapid STP または Multiple STP（MST）では、ポートの状態が転送に変更され、ロールが指定からルートに変更されると、トポロジが変更されることがあります。Rapid STP は、レイヤ 2 転送テーブルをただちにフラッシュします。802.1D はエージング タイムを短縮します。転送テーブルの即時フラッシュにより、接続はより高速に復元されますが、フラッディングが増加します。

安定したトポロジでは、トポロジを変更しても過剰なフラッディングは発生しません。リンクフラップはトポロジの変更を引き起こす可能性があるため、継続的なリンク フラップはトポロジの変更とフラッディングを繰り返す可能性があります。フラッディングはネットワーク パフォーマンスを低下させ、インターフェイスでパケット ドロップを引き起こす可能性があります。

手順の概要

1. switch# **show spanning-tree vlan** *vlan-id* **detail**

2. switch# **show spanning-tree vlan** *vlan-id* **detail**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	switch# **show spanning-tree vlan** *vlan-id* **detail**
	例：
	`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`
	`...`
		過剰なトポロジ変更の原因を判別します。

ステップ 2	switch# **show spanning-tree vlan** *vlan-id* **detail**
	例：
	`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`
	`  ...`
		トポロジ変更が発生したインターフェイスを特定します。
		トポロジの変更を開始したデバイスを分離できるようになるまで、インターフェイスに接続されているデバイスでこの手順を繰り返します。
		このデバイスのインターフェイスのリンク フラップを確認します。

コンバージェンス時間の問題のトラブルシューティング

STP のコンバージェンスに予想よりも長い時間がかかるか、予期しない最終的なネットワーク トポロジが発生する可能性があります。

コンバージェンスの問題をトラブルシューティングするには、次の問題を確認します。

- 文書化されたネットワーク トポロジ図のエラー。
- タイマーの設定ミス、直径、ブリッジ保証、ルート ガード、BPDU ガードなどのシスコ拡張機能など。
- 推奨論理ポート（ポート VLAN）の制限を超えたコンバージェンス中のスイッチ CPU の過負荷。
- STP に影響するソフトウェア障害。

フォワーディング ループに対するネットワークの保護

STP が特定の障害に正しく対処できないことを処理するために、シスコでは、ネットワークを転送ループから保護するための多数の機能と拡張機能を開発しました。

STP のトラブルシューティングは、特定の障害の原因を切り分けて見つけるのに役立ちますが、これらの拡張機能の実装は、ネットワークを転送ループから保護する唯一の方法です。

始める前に

- すべてのスイッチ間リンクでシスコ独自の単方向リンク検出（UDLD）プロトコルを有効にします。詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。
- 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 タイプとして設定して、ブリッジ保証機能を設定します。

（注） リンクの両側でブリッジ保証機能をイネーブルにする必要があります。そうでない場合は、Cisco NX-OS はブリッジ保証の不整合のためにポートがブロック状態になります。

- 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。

  STP エッジポートを設定して、ネットワークのパフォーマンスに影響を与える可能性のあるトポロジ変更通知および後続のフラッディングの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に接続するポートでのみ使用します。そうしないと、偶発

的なトポロジ ループによってデータ パケット ループが発生し、デバイスとネットワークの動作が中断される可能性があります。

- ポート チャネルの Link Aggregation Control Protocol（LACP）をイネーブルにして、ポート チャネルの設定ミスの問題を回避します。詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

  スイッチ間リンクで自動ネゴシエーションを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、リモート障害情報を伝達できます。これは、リモート側で障害を検出する最も迅速な方法です。リモート側で障害が検出されると、リンクがまだパルスを受信している場合でも、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場合は注意してください。STP タイマーは相互に依存しており、変更はネットワーク全体に影響を与える可能性があります。

手順の概要

1. （任意） switch(config)# **spanning-tree loopguard default**
2. switch(config)# **spanning-tree bpduguard enable**
3. switch(config)# **vlan** *vlan-range*
4. switch(config)# **spanning-tree vlan** *vlan-range* **root primary**
5. switch(config)# **spanning-tree vlan** *vlan-range* **root secondary**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） switch(config)# **spanning-tree loopguard default** 例： `switch(config)# spanning-tree loopguard default`	ルート ガードを使用してネットワーク STP 境界を保護します。ルート ガードと BPDU ガードを使用すると、外部からの影響から STP を保護できます。
ステップ 2	switch(config)# **spanning-tree bpduguard enable** 例： `switch(config)# spanning-tree bpduguard enable`	STP エッジポートで BPDU ガードをイネーブルにして、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、ブリッジング ルータなど）の影響を受けないようにします。 ルート ガードは、STP が外部の影響を受けないようにします。BPDU ガードは、BPDU（上位 BPDU だけでなく）を受信しているポートをシャットダウンします。 （注）

	コマンドまたはアクション	目的
		2 つの STP エッジ ポートが直接またはハブ経由で接続されている場合、短期間のループはルート ガードまたは BPDU ガードによって防止されません。
ステップ 3	switch(config)# **vlan** *vlan-range* 例： `switch(config)# vlan 9`	個別の VLAN を設定し、管理 VLAN でのユーザ トラフィックを回避します。管理 VLAN は、ネットワーク全体ではなくビルディング ブロックに含まれます。
ステップ 4	switch(config)# **spanning-tree vlan** *vlan-range* **root primary** 例： `switch(config)# spanning-tree vlan 9 root primary`	予測可能な STP ルートを設定します。
ステップ 5	switch(config)# **spanning-tree vlan** *vlan-range* **root secondary** 例： `switch(config)# spanning-tree vlan 12 root secondary`	予測可能なバックアップ STP ルート配置を設定します。 コンバージェンスが予測可能な方法で行われ、すべてのシナリオで最適なトポロジが構築されるように、STP ルートとバックアップ STP ルートを設定する必要があります。STP プライオリティをデフォルト値のままにしないでください。

翻訳について
このドキュメントは、米国シスコ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。