shutdown

インターフェイスをディセーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドを使用します。ディセーブルであるインターフェイスを再起動するには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートはイネーブルです（シャットダウンしません）。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

shutdown コマンドを入力すると、ポートは転送を停止します。ポートをイネーブルにするには、**no shutdown** コマンドを使用します。

削除、中断、またはシャットダウンされた VLAN に割り当てられているスタティック アクセス ポートに **no shutdown** コマンドを使用しても、無効です。ポートを再びイネーブルにするには、まずポートをアクティブ VLAN のメンバーにする必要があります。

shutdown コマンドは指定のインターフェイス上のすべての機能をディセーブルにします。

また、インターフェイスが使用不可であることをマーク付けします。インターフェイスがディセーブルかどうかを確認するには、**show interfaces** 特権 EXEC コマンドを使用します。シャットダウンされたインターフェイスは、管理上のダウンとして画面に表示されます。

例

次の例では、ポートをディセーブルにし、次に再びイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	すべてのインターフェイスまたは特定のインターフェイスに対する統計情報を表示します。

shutdown vlan

指定された VLAN 上のローカル トラフィックをシャットダウン（一時停止）するには、**shutdown vlan** グローバル コンフィギュレーション コマンドを使用します。VLAN 上のローカル トラフィックを再開する場合は、このコマンドの **no** 形式を使用します。

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

シンタックスの説明

vlan-id	ローカルにシャットダウンする VLAN の ID です。指定できる範囲は 2 ～ 1001 です。VLAN トランキング プロトコル（VTP）環境のデフォルト VLAN として定義された VLAN と ID が 1005 より大きい拡張範囲 VLAN はシャットダウンできません。デフォルト VLAN は 1 および 1002 ～ 1005 です。

デフォルト

デフォルトは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

shutdown vlan コマンドは、VTP データベース内の VLAN 情報を変更しません。このコマンドはローカル トラフィックをシャットダウンしますが、スイッチは VTP 情報をアドバタイズし続けます。

例

次の例では、VLAN 2 のトラフィックをシャットダウンする方法を示します。

```
Switch(config)# shutdown vlan 2
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
shutdown（config-vlan モード）	config-vlan モード（**vlan** *vlan-id* グローバル コンフィギュレーション コマンドで開始）の場合に、VLAN のローカル トラフィックをシャットダウンします。
vlan database	VLAN コンフィギュレーション モードを開始します。

small-frame violation rate

指定されたレートで小さいフレーム（67 バイト以下）の VLAN タグ付きパケットを受信した場合にインターフェイスが errdisable になるレート（しきい値）を設定するには、**small-frame violation rate** ***pps*** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

small-frame violation rate *pps*

no small-frame violation rate *pps*

シンタックスの説明

pps	小さいフレームを受信したインターフェイスが errdisable になるしきい値を指定します。範囲は、1 ～ 10,000 pps です。

デフォルト

この機能は、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(44)SE	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、小さいフレームを受信したときにポートが errdisable になるレート（しきい値）をイネーブルにします。小さいフレームは、67 以下のフレームと考えられます。

各ポートの小さいフレームのしきい値をグローバルにイネーブルにするには、**errdisable detect cause small-frame** グローバル コンフィギュレーション コマンドを使用します。

errdisable recovery cause small-frame グローバル コンフィギュレーション コマンドを使用して、ポートが自動的に再びイネーブルになるように設定できます。**errdisable recovery interval** *interval グローバル コンフィギュレーション コマンド*を使用して、回復時間を設定します。

例

次の例では、小さなフレームが 10,000 pps で着信した場合にポートを errdisable にする小さいフレームの着信レート機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# small-frame violation rate 10000
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable detect cause small-frame	着信フレームが最小サイズより小さく、指定されたレート（しきい値）で着信する場合に、スイッチ ポートが errdisable ステートになるようにします。
errdisable recovery cause small-frame	復旧タイマーをイネーブルにします。
show interfaces	入出力フロー制御を含むスイッチのインターフェイス設定を表示します。

snmp-server enable traps

スイッチでさまざまなトラップの簡易ネットワーク管理プロトコル（SNMP）通知を送信したり、ネットワーク管理システム（NMS）に要求を通知したりできるようにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **copy-config** | **cpu threshold** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **errdisable [notification-rate value]** | **flash** | **ipmulticast** | **mac-notification** | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**] | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp]**

no snmp-server enable traps [**bridge** [**newroot**] [**topologychange**] | **cluster** | **config** | **copy-config** | **cpu threshold** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **errdisable [notification-rate]** | **flash** | **ipmulticast** | **mac-notification** | **msdp** | **ospf** [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**] | **pim** [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**] | **port-security** [**trap-rate**] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vtp**]

シンタックスの説明

bridge [**newroot**] [**topologychange**]	（任意）スパニングツリー プロトコル（STP）ブリッジ MIB（管理情報ベース）トラップを生成します。キーワードの意味は次のとおりです。 • **newroot**：（任意）SNMP STP ブリッジ MIB の新しいルート トラップをイネーブルにします。 • **topologychange**：（任意）SNMP STP ブリッジ MIB のトポロジ変更トラップをイネーブルにします。
cluster	（任意）クラスタ トラップをイネーブルにします。
config	（任意）SNMP 設定トラップをイネーブルにします。
copy-config	（任意）SNMP コピー設定トラップをイネーブルにします。
cpu threshold	（任意）CPU に関連したトラップをイネーブルにします。 このキーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。
entity	（任意）SNMP エンティティ トラップをイネーブルにします。

envmon [**fan** | **shutdown** | **status** | **supply** | **temperature**]	（任意）SNMP 環境トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **fan**：（任意）ファン トラップをイネーブルにします。 • **shutdown**：（任意）環境モニタ シャットダウン トラップをイネーブルにします。 • **status**：（任意）SNMP 環境ステータス変更トラップをイネーブルにします。 • **supply**：（任意）環境モニタ電源トラップをイネーブルにします。 • **temperature**：（任意）環境モニタ温度トラップをイネーブルにします。
errdisable [**notification-rate** *value*]	（任意）errdisable トラップをイネーブルにします。notification-rate キーワードを使用して、毎分送信される errdisable トラップの最大値を設定します。指定できる範囲は 0 ～ 10000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。
flash	（任意）SNMP FLASH 通知をイネーブルにします。
ipmulticast	（任意）IP マルチキャスト ルーティング トラップをイネーブルにします。
mac-notification	（任意）MAC（メディア アクセス制御）アドレス通知トラップをイネーブルにします。
msdp	（任意）Multicast Source Discovery Protocol（MSDP）トラップをネーブルにします。
ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]	（任意）Open Shortest Path First（OSPF）トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **cisco-specific**：（任意）シスコ固有のトラップをイネーブルにします。 • **errors**：（任意）エラー トラップをイネーブルにします。 • **lsa**：（任意）Link-State Advertisement（LSA; リンクステートアドバタイズメント）トラップをイネーブルにします。 • **rate-limit**：（任意）速度制限トラップをイネーブルにします。 • **retransmit**：（任意）パケット再送信トラップをイネーブルにします。 • **state-change**：（任意）ステート変更トラップをイネーブルにします。
pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]	（任意）Protocol-Independent Multicast（PIM）トラップをネーブルにします。キーワードの意味は次のとおりです。 • **invalid-pim-message**：（任意）無効な PIM メッセージ トラップをイネーブルにします。 • **neighbor-change**：（任意）PIM ネイバー変更トラップをイネーブルにします。 • **rp-mapping-change**：（任意）Rendezvous Point（RP）マッピング変更トラップをイネーブルにします。
port-security [**trap-rate** *value*]	（任意）ポート セキュリティ トラップをイネーブルにします。1 秒間に送信するポート セキュリティ トラップの最大数を設定するには、**trap-rate** キーワードを使用します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0（制限はなく、トラップをすべての発生原因にたいして送信）です。
rtr	（任意）SNMP Response Time Reporter トラップをイネーブルにします。 このキーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。

snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	（任意）SNMP トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **authentication**：（任意）認証トラップをイネーブルにします。 • **coldstart**：（任意）コールド スタート トラップをイネーブルにします。 • **linkdown**：（任意）リンクダウン トラップをイネーブルにします。 • **linkup**：（任意）リンクアップ トラップをイネーブルにします。 • **warmstart**：（任意）ウォーム スタート トラップをイネーブルにします。
storm-control trap-rate *value*	（任意）ストーム制御トラップをイネーブルにします。分単位で送信されるストーム制御トラップの最大数を設定するには、**trap-rate** キーワードを使用します。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。
stpx	（任意）SNMP STPX MIB トラップをイネーブルにします。キーワードの意味は次のとおりです。 • **inconsistency**：（任意）SNMP STPX MIB の矛盾更新トラップをイネーブルにします。 • **root-inconsistency**：（任意）SNMP STPX MIB のルート矛盾更新トラップをイネーブルにします。 • **loop-inconsistency**：（任意）SNMP STPX MIB のループ矛盾更新トラップをイネーブルにします。
Syslog	（任意）SNMP Syslog トラップをイネーブルにします。
tty	（任意）TCP 接続トラップを送信します。デフォルトでイネーブルになっています。
vlan-membership	（任意）SNMP VLAN メンバシップ トラップをイネーブルにします。
vlancreate	（任意）SNMP VLAN 作成トラップをイネーブルにします。
vlandelete	（任意）SNMP VLAN 削除トラップをイネーブルにします。
vtp	（任意）VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）トラップをイネーブルにします。

（注） **hsrp**、**insertion**、**removal**、および **rtr** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP 情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	**errdisable notification-rate** *value* キーワードが追加されました。
12.2(50)SE	**cpu threshold** キーワードが追加されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

snmp-server enable traps コマンドは、トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにします。

（注）　SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

CPU しきい値通知のタイプと値を設定するには、**process cpu threshold type** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、NMS に VTP トラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps vtp
```

設定を確認するには、**show vtp status** 特権 EXEC コマンド、または **show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
snmp-server host	SNMP トラップを受信するホストを指定します。

snmp-server host

SNMP 通知処理の受信側（ホスト）を指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用します。指定されたホストを削除するには、このコマンドの **no** 形式を使用します。

snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth**| **priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

no snmp-server host *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}] [**vrf** *vrf-instance*] *community-string*

シンタックスの説明

host-addr	ホストの名前またはインターネット アドレス（ターゲットとなる受信側）です。
udp-port *port*	（任意）トラップを受信するホストの User Datagram Protocol（UDP）ポート番号を設定します。指定できる範囲は 0 ～ 65535 です。
informs | **traps**	（任意）このホストに SNMP トラップまたは情報を送信します。
version 1 | **2c** | **3**	（任意）トラップの送信に使用する SNMP のバージョンです。 次のキーワードがサポートされています。 **1**：SNMPv1。情報の場合は、このオプションを使用できません。 **2c**：SNMPv2C。 **3**：SNMPv3。バージョン 3 キーワードのあとに、次に示すオプション キーワードを指定できます。 • **auth**（任意）：MD5 および Secure Hash Algorithm（SHA）によるパケット認証をイネーブルにします。 • **noauth**（デフォルト）：noAuthNoPriv というセキュリティ レベルです。[**auth** | **noauth** | **priv**] キーワードが指定されていない場合は、これがデフォルトです。 • **priv**（任意）：Data Encryption Standard（DES; データ暗号化規格）によるパケット暗号化（*プライバシ*ともいう）をイネーブルにします。 （注）　**priv** キーワードは、暗号化ソフトウェア イメージがインストールされている場合にだけ利用できます。
vrf *vrf-instance*	（任意）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）ルーティング インスタンスとホスト名です。

community-string	通知処理によって送信されるパスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用し、次に **snmp-server host** コマンドを使用することを推奨します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定する場合は、SNMP コミュニティ ストリングとして @ 記号を使用しないようにしてください。

notification-type　（任意）ホストに送信される通知のタイプ。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの 1 つまたは複数を指定できます。

- **bridge**：（任意）SNMP スパニングツリー プロトコル（STP）ブリッジ MIB トラップを送信します。
- **cluster**：クラスタ メンバー ステータス トラップを送信します。
- **config**：SNMP 設定トラップを送信します。
- **copy-config**：SNMP コピー設定トラップを送信します。
- **cpu threshold**：CPU に関連したトラップを許可します。このキーワードを使用できるのは、スイッチで LAN Base イメージが実行されている場合だけです。
- **entity**：SNMP エンティティ トラップを送信します。
- **envmon**：環境モニタ トラップを送信します。
- **errdisable**：SNMP errdisable 通知を送信します。
- **flash**：SNMP FLASH 通知を送信します。
- **hsrp**：SNMP Hot Standby Router Protocol（HSRP）トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **mac-notification**：SNMP MAC（メディア アクセス制御）通知トラップを送信します。
- **msdp**：SNMP Multicast Source Discovery Protocol（MSDP）トラップを送信します。
- **ospf**：Open Shortest Path First（OSPF）トラップを送信します。
- **pim**：SNMP Protocol-Independent Multicast（PIM）トラップを送信します。
- **port-security**：SNMP ポートセキュリティ トラップを送信します。
- **rtr**：SNMP Response Time Reporter トラップを送信します。
- **snmp**：SNMP タイプ トラップを送信します。
- **storm-control**：SNMP ストーム制御トラップを送信します。
- **stpx**：SNMP STP 拡張 MIB トラップを送信します。
- **syslog**：SNMP Syslog トラップを送信します。
- **tty**：TCP 接続トラップを送信します。
- **udp-port** *port*：トラップを受信するホストの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号を設定します。指定できる範囲は 0 ～ 65535 です。
- **vlan-membership**：SNMP VLAN メンバシップ トラップを送信します。
- **vlancreate**：SNMP VLAN 作成トラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vtp**：SNMP VLAN トランキング プロトコル（VTP）トラップを送信します。

デフォルト

このコマンドは、デフォルトではディセーブルです。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップ タイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで **noauth**（noAuthNoPriv）セキュリティ レベルになります。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(37)SE	**errdisable notification-rate** *value* キーワードが追加されました。
12.2(50)SE	**cpu threshold** キーワードが追加されました。

使用上のガイドライン

SNMP 通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送Mしないため、トラップは信頼できません。送信側は、トラップが受信されたかどうかを判別できません。ただし、情報要求を受信した SNMP エンティティは、SNMP 応答 PDU を使用してメッセージに確認応答します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。したがって、情報が目的の宛先に到達する可能性が高まります。

ただし、情報はエージェントおよびネットワークのリソースをより多く消費します。送信と同時にドロップされるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は 1 回限りですが、情報は数回にわたって再試行が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなります。

snmp-server host コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するようにスイッチを設定するには、少なくとも 1 つの **snmp-server host** コマンドを入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合は、ホストに対してすべてのトラップ タイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。ホストごとのコマンドでは、複数の通知タイプを指定できます。

ローカル ユーザがリモート ホストと関連付けられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知に対して複数の **snmp-server host** コマンドを指定した場合は、あとのコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドのみが有効です。たとえば、ホストに **snmp-server host inform** を入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番めのコマンドによって最初のコマンドが置き換えられます。

snmp-server host コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。1 つのホストが大部分の通知を受信する場合は、このホストに対して、少なくとも 1 つの **snmp-server enable traps** コマンドおよび **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブル化されます。

キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング *comaccess* を設定し、このストリングによる、アクセスリスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

次の例では、名前 *myhost.cisco.com* で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、*comaccess* として定義されています。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ ストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする方法を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
snmp-server enable traps	各トラップ タイプまたは情報要求の SNMP 通知をイネーブルにします。

snmp trap mac-notification

特定のレイヤ 2 インターフェイス上で SNMP MAC アドレス通知トラップをイネーブルにするには、**snmp trap mac-notification** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp trap mac-notification {**added | removed**}

no snmp trap mac-notification {**added | removed**}

シンタックスの説明

added	MAC アドレスがインターフェイスに追加されるたびに、MAC 通知トラップをイネーブルにします。
removed	MAC アドレスがインターフェイスから削除されるたびに、MAC 通知トラップをイネーブルにします。

デフォルト

デフォルトでは、アドレス追加および削除に対するトラップは両方ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

snmp trap mac-notification コマンドを使用して、特定のインターフェイスの通知トラップをイネーブルにできますが、トラップが生成されるのは、**snmp-server enable traps mac-notification** および **mac address-table notification** グローバル コンフィギュレーション コマンドをイネーブルにした場合のみです。

例

次の例では、MAC アドレスがポートに追加されたときに MAC 通知トラップをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification added
```

設定を確認するには、**show mac address-table notification interface** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear mac address-table notification	MAC アドレス通知グローバル カウンタをクリアします。
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
show mac address-table notification	**interface** キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp-server enable traps	**mac-notification** キーワードが追加された場合に SNMP MAC 通知トラップを送信します。

spanning-tree backbonefast

BackboneFast 機能をイネーブルにするには、**spanning-tree backbonefast** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree backbonefast

no spanning-tree backbonefast

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

BackboneFast はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

BackboneFast 機能は、Rapid PVST+ または Multiple Spanning-Tree（MST）モード用に設定できますが、スパニングツリー モードを PVST+ に変更するまでこの機能はディセーブル（非アクティブ）のままです。

スイッチのルート ポートまたはブロックされたポートが、指定されたスイッチから不良ブリッジ プロトコル データ ユニット（BPDU）を受信すると、BackboneFast が開始されます。下位 BPDU は、ルート ブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位 BPDU を受信した場合、そのスイッチが直接接続されていないリンク（*間接*リンク）で障害が発生したことを意味します（指定スイッチとルート スイッチ間の接続が切断されています）。ルート スイッチへの代替パスがある場合に BackboneFast を使用すると、不良 BPDU を受信するインターフェイスの最大エージング タイムが期限切れになり、ブロックされたポートをただちにリスニング ステートに移行できます。そのあと、BackboneFast はインターフェイスをフォワーディング ステートに移行させます。詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

間接リンク障害を検出できるようにしたり、スパニングツリーの再認識をより短時間で開始したりするには、サポートされるすべてのスイッチで BackboneFast をイネーブルにしてください。

例

次の例では、スイッチ上で BackboneFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree backbonefast
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。

spanning-tree bpdufilter

インターフェイス上での BPDU の送受信を禁止するには、**spanning-tree bpdufilter** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

シンタックスの説明

disable	指定されたインターフェイス上で BPDU フィルタリングをディセーブルにします。
enable	指定されたインターフェイス上で BPDU フィルタリングをイネーブルにします。

デフォルト

BPDU フィルタリングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、BPDU フィルタリング機能をイネーブルにできます。

注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

すべての PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにするには、**spanning-tree portfast bpdufilter default** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpdufilter** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポート上で BPDU フィルタリング機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree bpduguard

BPDU を受信したインターフェイスを errdisable ステートにするには、**spanning-tree bpduguard** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

シンタックスの説明

disable	指定されたインターフェイス上で BPDU ガードをディセーブルにします。
enable	指定されたインターフェイス上で BPDU ガードをイネーブルにします。

デフォルト

BPDU ガードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスを手動で再び動作する必要がある場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でインターフェイスがスパニングツリー トポロジに追加されないようにするには、BPDU ガード機能を使用します。

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、BPDU ガード機能をイネーブルにできます。

すべての PortFast 対応インターフェイス上で BPDU ガードをグローバルにイネーブルにするには、**spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bpduguard** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ポートで BPDU ガード機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	特定のインターフェイスおよび対応するすべての VLAN 上で、PortFast 機能をイネーブルにします。

spanning-tree cost

スパニングツリーの計算に使用するパス コストを設定するには、**spanning-tree cost** インターフェイス コンフィギュレーション コマンドを使用します。ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

シンタックスの説明

vlan *vlan-id*	（任意）スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ～ 4094 です。
cost	パス コスト。使用できる範囲は 1 ～ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s : 4
- 100 Mb/s : 19
- 10 Mb/s : 100

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

spanning-tree vlan *vlan-id* **cost** *cost* コマンドおよび **spanning-tree cost** *cost* コマンドの両方を使用してインターフェイスを設定する場合、**spanning-tree vlan** *vlan-id* **cost** *cost* コマンドが有効になります。

例

次の例では、ポートでパス コストを 250 に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

次の例では、VLAN 10、12 ～ 15、および 20 に対してパス コスト 300 を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

設定を確認するには、**show spanning-tree interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー情報を表示します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree etherchannel guard misconfig

スイッチが EtherChannel の設定ミスを検出した場合にエラーメッセージを表示するには、**spanning-tree etherchannel guard misconfig** グローバル コンフィギュレーション コマンドを使用します。機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

EtherChannel ガードはスイッチでイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが EtherChannel の設定ミスを検出すると、次のエラー メッセージが表示されます。

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

設定ミスの EtherChannel にあるスイッチ ポートを表示するには、**show interfaces status err-disabled** 特権 EXEC コマンドを使用します。リモート デバイスの EtherChannel 設定を確認するには、リモート デバイスで **show etherchannel summary** 特権 EXEC コマンドを使用します。

EtherChannel の設定矛盾によりポートが errdisable ステートの場合は、**errdisable recovery cause channel-misconfig** グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して、手動で再度イネーブルにすることができます。

例

次の例では、EtherChannel ガードの設定ミス機能をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
errdisable recovery cause channel-misconfig	EtherChannel の設定矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
show etherchannel summary	チャネルの EtherChannel 情報を、チャネルグループ単位で 1 行のサマリーとして表示します。
show interfaces status err-disabled	errdisable ステートのインターフェイスを表示します。

spanning-tree extend system-id

拡張システム ID 機能をイネーブルにするには、**spanning-tree extend system-id** グローバル コンフィギュレーション コマンドを使用します。

spanning-tree extend system-id

（注）　このコマンドの **no** バージョンは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。拡張システム ID 機能をディセーブルにすることはできません。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

拡張システム ID はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチは、IEEE 802.1t スパニングツリー拡張をサポートします。以前スイッチ プライオリティに使用されたビットの一部は現在、拡張システム ID（Per-VLAN Spanning-Tree Plus [PVST+] と Rapid PVST+ の VLAN 識別子、または Multiple Spanning-Tree [MST] のインスタンス識別子）に使用します。

スパニングツリーは、ブリッジ ID が VLAN または MST インスタンスごとに一意となるようにするために、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパニングツリー MAC アドレスを使用しています。

拡張システム ID のサポートにより、ルート スイッチ、セカンダリ ルート スイッチ、および VLAN のスイッチ プライオリティを手動で設定する方法に影響が生じます。詳細については、「spanning-tree mst root」および「spanning-tree vlan」を参照してください。

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルート スイッチになることはほぼありません。拡張システム ID によって、接続されたスイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチ プライオリティ値が増大します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree guard

選択したインターフェイスに関連付けられたすべての VLAN 上でルート ガードまたはループ ガードをイネーブルにするには、**spanning-tree guard** インターフェイス コンフィギュレーション コマンドを使用します。ルート ガードは、スパニングツリー ルート ポートまたはスイッチのルートへのパスになることが可能なインターフェイスを制限します。ループ ガードは、障害によって単一方向リンクが作成された場合に、代替ポートまたはルート ポートが指定ポートにならないようにします。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree guard {**loop** | **none** | **root**}

no spanning-tree guard

シンタックスの説明

loop	ループ ガードをイネーブルにします。
none	ルート ガードまたはループ ガードをディセーブルにします。
root	ルート ガードをイネーブルにします。

デフォルト

ルート ガードはディセーブルです。

ループ ガードは、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドに従って設定されます（グローバルにディセーブル化）。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、ルート ガードまたはループ ガード機能をイネーブルにできます。

ルート ガードがイネーブルの場合に、スパニングツリーを計算すると、インターフェイスがルート ポートとして選択され、root-inconsistent（ブロック）ステートに移行します。これにより、カスタマーのスイッチがルート スイッチになったり、ルートへのパスになったりすることがなくなります。ルート ポートは、スイッチからルート スイッチまでの最適パスを提供します。

no spanning-tree guard または **no spanning-tree guard none** コマンドを入力すると、ルート ガードは選択されたインターフェイスのすべての VLAN でディセーブルになります。このインターフェイスが root-inconsistent（ブロック）ステートの場合、インターフェイスはリスニング ステートに自動的に移行します。

UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）になり、フォワーディング ステートに移行できなくなります。スイッチが Rapid PVST+ モードまたは MST モードで稼動している場合は、UplinkFast 機能は使用できません。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid PVST+ モードで稼動している場合は、ループ ガードによって代替ポートとルート ポートが指定のポートにならなくなり、スパニングツリーによって代替ポート上でもルート ポート上でも BPDU が送信されなくなります。スイッチが MST モードで稼動している場合は、すべての MST インスタンスでこのインターフェイスがループ ガードによってブロックされている場合のみ、非境界インターフェイスから BPDU が送信されなくなります。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ルート ガードまたはループ ガードをディセーブルにする場合は、**spanning-tree guard none** インターフェイス コンフィギュレーション コマンドを使用します。ルート ガードとループ ガードの両方を同時にイネーブルにすることはできません。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、指定のポートに関連付けられたすべての VLAN で、ルート ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

次の例では、指定のポートに関連付けられたすべての VLAN 上でループ ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree loopguard default	単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートとして使用されないようにします。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst root	ネットワークの直径に基づいて、MST ルート スイッチのプライオリティおよびタイマーを設定します。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree link-type

インターフェイスのデュプレックス モードによって決まるデフォルトのリンクタイプ設定を無効化し、フォワーディング ステートへの高速スパニングツリーの移行をイネーブルにするには、**spanning-tree link-type** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

シンタックスの説明

point-to-point	インターフェイスのリンク タイプがポイントツーポイントであることを指定します。
shared	インターフェイスのリンク タイプが共有であることを指定します。

デフォルト

スイッチは、デュプレックス モードからインターフェイスのリンク タイプを取得します。つまり、全二重インターフェイスはポイントツーポイント リンクであると見なされ、半二重インターフェイスは共有リンクであると見なされます。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

リンク タイプのデフォルト設定を上書きするには、**spanning-tree link-type** コマンドを使用します。たとえば、半二重リンクは、Multiple Spanning-Tree Protocol（MSTP）または Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルが稼動し高速移行がイネーブルであるリモート スイッチの 1 つのインターフェイスに、ポイントツーポイントで物理的に接続できます。

例

次の例では、（デュプレックスの設定に関係なく）リンク タイプを共有に指定し、フォワーディング ステートへの高速移行を禁止する方法を示します。

```
Switch(config-if)# spanning-tree link-type shared
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* または show **spanning-tree interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear spanning-tree detected-protocols	すべてのインターフェイスまたは指定されたインターフェイスでプロトコル移行プロセスを再開（強制的に近接スイッチと再びネゴシエートさせる）します。
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー ステート情報を表示します。
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。

spanning-tree loopguard default

単一方向リンクを発生させる障害が原因で代替ポートまたはルート ポートが指定のポートになることを防ぐには、**spanning-tree loopguard default** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree loopguard default

no spanning-tree loopguard default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ループ ガードはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid-PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、ループ ガード機能をイネーブルにできます。

ループ ガード機能は、スイッチド ネットワーク全体に設定した場合に最も効果があります。スイッチが PVST+ モードまたは Rapid PVST+ モードで稼動している場合、ループ ガードによって、代替ポートおよびルート ポートは指定ポートになることがなく、スパニング ツリーはルートポートまたは代替ポートでブリッジ プロトコル データ ユニット（BPDU）を送信しません。スイッチが MST モードで稼動している場合は、すべての MST インスタンスでこのインターフェイスがループ ガードによってブロックされている場合のみ、非境界インターフェイスから BPDU が送信されなくなります。境界インターフェイスでは、ループ ガードによってすべての MST インスタンスでインターフェイスがブロックされます。

ループ ガードは、スパニング ツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。

spanning-tree loopguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree guard loop** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、ループ ガードをグローバルにイネーブルにします。

```
Switch(config)# spanning-tree loopguard default
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree guard loop	指定したインターフェイスに関連付けられたすべての VLAN で、ループ ガード機能をイネーブルにします。

spanning-tree mode

スイッチ上で Per-VLAN Spanning-Tree Plus（PVST+）、Rapid-PVST+、または Multiple Spanning-Tree（MST）をイネーブルにするには、**spanning-tree mode** + グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mode {**mst** | **pvst** | **rapid-pvst**}

no spanning-tree mode

シンタックスの説明

mst	MST および Rapid Spanning-Tree Protocol（RSTP）をイネーブルにします（IEEE 802.1s および IEEE 802.1w に準拠）。
pvst	PVST+ をイネーブルにします（IEEE 802.1D に準拠）。
rapid-pvst	Rapid-PVST+ をイネーブルにします（IEEE 802.1w に準拠）。

デフォルト

デフォルト モードは PVST+ です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチは PVST+、Rapid PVST+、および MSTP をサポートしていますが、常時アクティブにできるのは 1 つのバージョンだけです。すべての VLAN で PVST+ が実行されるか、すべての VLAN で Rapid-PVST+ が実行されるか、またはすべての VLAN で MSTP が実行されます。

MST モードをイネーブルにした場合、RSTP が自動的にイネーブルになります。

注意　スパニングツリー モードを変更すると、すべてのスパニングツリー インスタンスが以前のモードのために停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。

例

次の例では、スイッチ上で MST および RSTP をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode mst
```

次の例では、スイッチ上で Rapid-PVST+ をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree mode rapid-pvst
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。

spanning-tree mst configuration

Multiple Spanning-Tree（MST）リージョンを設定する場合に使用する MST コンフィギュレーション モードを開始するには、**spanning-tree mst configuration** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst configuration

no spanning-tree mst configuration

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべての VLAN（仮想 LAN）が Common and Internal Spanning-Tree（CIST）インスタンス（インスタンス 0）にマッピングされます。

デフォルト名は空の文字列です。

リビジョン番号は 0 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

MST コンフィギュレーション モードをイネーブルにするには、**spanning-tree mst configuration** コマンドを使用します。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **abort** : 設定変更を適用せずに MST リージョン コンフィギュレーション モードを終了します。
- **exit** : MST リージョン コンフィギュレーション モードを終了し、すべての設定変更を適用します。
- **instance** *instance-id* **vlan** *vlan-range* : VLAN を MST インスタンスにマッピングします。指定できる *instance-id* の範囲は 1 ～ 4094 です。指定できる *vlan-range* の範囲は 1 ～ 4094 です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。
- **name** *name* : 設定名を指定します。*name* ストリングには最大 32 文字まで使用でき、大文字と小文字が区別されます。
- **no** : **instance**、**name**、および **revision** コマンドを無視するか、またはデフォルト設定に戻します。
- **private-vlan** : このコマンドは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。
- **revision** *version* : 設定のリビジョン番号を指定します。指定できる範囲は 0 ～ 65535 です。
- **show** [**current** | **pending**] : 現在の MST リージョン設定または保留中の MST リージョン設定を表示します。

MST モードでは、スイッチは最大 65 の MST インスタンスまでサポートします。特定の MST インスタンスにマッピング可能な VLAN 数は制限されていません。

VLAN を MST インスタンスにマッピングすると、マッピングは差分で実行され、コマンドで指定された VLAN が以前マッピングされた VLAN に追加または VLAN から削除されます。範囲を指定する場合は、ハイフンを使用します。たとえば、**instance 1 vlan 1-63** と指定すると、MST インスタンス 1 に VLAN 1 ～ 63 がマッピングされます。列挙を指定する場合は、カンマを使用します。たとえば、**instance 1 vlan 10, 20, 30** と指定すると、MST インスタンス 1 に VLAN 10、20、および 30 がマッピングされます。

明示的に MST インスタンスにマッピングされていないすべての VLAN は、CIST インスタンス（インスタンス 0）にマッピングされます。このマッピングは、このコマンドの **no** 形式では解除できません。

2 台以上のスイッチが同一 MST リージョン内に存在するには、同じ VLAN マッピング、同じ構成リビジョン番号、および同じ名前が設定されている必要があります。

例

次の例では、MST コンフィギュレーション モードを開始して VLAN 10 ～ 20 を MST インスタンス 1 にマッピングし、リージョンに *region1* と名前を付けて、構成リビジョンを 1 に設定します。変更確認前の構成を表示して変更を適用し、グローバル コンフィギュレーション モードに戻る方法を示します。

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

次の例では、インスタンス 2 にすでにマッピングされている VLAN があれば、そこに VLAN 1 ～ 100 を追加し、インスタンス 2 にマッピングされていた VLAN 40 ～ 60 を CIST インスタンスに移動し、インスタンス 10 に VLAN 10 を追加し、インスタンス 2 にマッピングされたすべての VLAN を削除し、それらを CIST インスタンスにマッピングする方法を示します。

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

設定を確認するには、**show pending** MST コンフィギュレーション コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst configuration	MST リージョンの設定を表示します。

spanning-tree mst cost

Multiple Spanning-Tree（MST）の計算に使用するパス コストを設定するには、**spanning-tree mst cost** インターフェイス コンフィギュレーション コマンドを使用します。ループが発生した場合、スパニング ツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

シンタックスの説明

instance-id	スパニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ～ 4094 です。
cost	パス コストの範囲は 1 ～ 200000000 です。値が大きいほど、コストが高くなります。

デフォルト

デフォルト パス コストは、インターフェイス帯域幅の設定から計算されます。IEEE のデフォルト パス コスト値は、次のとおりです。

- 1000 Mb/s：20000
- 100 Mb/s：200000
- 10 Mb/s：2000000

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

コストを設定する場合は、値が大きいほどコストが高くなります。

例

次の例では、インスタンス 2 および 4 に関連付けられたポートにパス コストとして 250 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。
spanning-tree mst priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst forward-time

すべての Multiple Spanning-Tree（MST）インスタンスの転送遅延時間を設定するには、**spanning-tree mst forward-time** グローバル コンフィギュレーション コマンドを使用します。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を指定します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

シンタックスの説明

seconds	リスニングおよびラーニング ステートの期間です。指定できる範囲は 4 ～ 30 秒です。

デフォルト

デフォルト値は 15 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst forward-time コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての MST インスタンスについて、スパニングツリーの転送時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst forward-time 18
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージから送信される hello BPDU（ブリッジ プロトコル データ ユニット）の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst hello-time

ルート スイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔を設定するには、**spanning-tree mst hello-time** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

シンタックスの説明

seconds	ルート スイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔です。指定できる範囲は 1 ～ 10 秒です。

デフォルト

デフォルト値は 2 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst max-age *seconds* グローバル コンフィギュレーション コマンドを設定したあとに、指定された期間内にルート スイッチから BPDU を受信しない場合、スイッチはスパニングツリー トポロジを再計算します。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst hello-time コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての MST インスタンスについて、スパニングツリーの hello タイムを 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst hello-time 3
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst max-age

スパニングツリーがルート スイッチからメッセージを受信する間隔を設定するには、**spanning-tree mst max-age** グローバル コンフィギュレーション コマンドを使用します。スイッチがこのインターバル内にルート スイッチからブリッジ プロトコル データ ユニット（BPDU）メッセージを受信しない場合は、スパニングツリー トポロジが再計算されます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

シンタックスの説明

seconds	スパニング ツリーがルート スイッチからメッセージを受信する間隔です。指定できる範囲は 6 ～ 40 秒です。

デフォルト

デフォルト値は 20 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

spanning-tree mst max-age *seconds* グローバル コンフィギュレーション コマンドを設定したあとに、指定された期間内にルート スイッチから BPDU を受信しない場合、スイッチはスパニングツリー トポロジを再計算します。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree mst max-age コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニングツリーの有効期間を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-age 30
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。

コマンド	説明
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree mst max-hops

BPDU が廃棄されて、インターフェイスに保持された情報が期限切れになるまでのリージョンのホップ数を設定するには、**spanning-tree mst max-hops** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

シンタックスの説明

hop-count	BPDU が廃棄されるまでのリージョンのホップ数です。指定できるホップ数は 1 ～ 255 です。

デフォルト

デフォルトのホップ数は 20 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*hop-count* の範囲は 1 ～ 255 に変更されました。

使用上のガイドライン

インスタンスのルート スイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。スイッチは、BPDU を受信すると、受信した残りのホップ カウントを 1 つ減らして、生成する M レコードの残りのホップ カウントとしてこの値を伝播します。ホップ カウントが 0 になると、スイッチは BPDU を廃棄して、インターフェイスに保持された情報を期限切れにします。

spanning-tree mst max-hops コマンドを変更すると、すべてのスパニングツリー インスタンスに影響します。

例

次の例では、すべての Multiple Spanning-Tree（MST）インスタンスについて、スパニングツリーの最大ホップ数を 10 に設定する方法を示します。

```
Switch(config)# spanning-tree mst max-hops 10
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。

spanning-tree mst port-priority

インターフェイス プライオリティを設定するには、**spanning-tree mst port-priority** インターフェイス コンフィギュレーション コマンドを使用します。ループが発生した場合、Multiple Spanning-Tree Protocol（MSTP）はフォワーディング ステートに設定するインターフェイスを判別できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

シンタックスの説明

instance-id	スパニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ～ 4094 です。
priority	指定できる範囲は 0 ～ 240 であり、刻み幅は 16 です。有効なプライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

最初に選択させるインターフェイスには高いプライオリティ（小さい数値）を与え、最後に選択させるインターフェイスには低いプライオリティ（大きい数値）を付けます。すべてのインターフェイスに同じプライオリティ値が付けられている場合、Multiple Spanning-Tree（MST）はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

例

次の例では、ループが発生した場合に、スパニングツリー インスタンス 20 および 22 に関連付けられたインターフェイスがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

設定を確認するには、**show spanning-tree mst interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst interface *interface-id*	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree mst pre-standard

ポートが先行標準ブリッジ プロトコル データ ユニット（BPDU）のみを送信するように設定するには、**spanning-tree mst pre-standard** インターフェイス コンフィギュレーション コマンドを使用します。

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

デフォルトのステートは、先行標準ネイバーの自動検出です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

ポートでは、先行標準と標準の両方の BPDU を受け入れることができます。ネイバー タイプが不一致の場合、Common and Internal Spanning-Tree（CIST）のみがこのインターフェイスで実行されます。

（注）スイッチのポートが、先行標準の Cisco IOS ソフトウェアを実行しているスイッチに接続されている場合には、ポートに対して **spanning-tree mst pre-standard** インターフェイス コンフィギュレーション コマンドを使用する*必要があります*。ポートが先行標準 BPDU のみを送信するように設定していない場合、Multiple STP（MSTP）のパフォーマンスが低下することがあります。

自動的に先行標準ネイバーを検出するようにポートが設定されている場合、**show spanning-tree mst** コマンドに *prestandard* フラグが常に表示されます。

例

次の例では、ポートが先行標準 BPDU のみを送信するように設定する方法を示します。

```
Switch(config-if)# spanning-tree mst pre-standard
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	*prestandard* フラグなど、指定されたインターフェイスの Multiple Spanning-Tree（MST）情報を表示します。

spanning-tree mst priority

指定されたスパニングツリー インスタンスに対してスイッチのプライオリティを設定するには、**spanning-tree mst priority** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

シンタックスの説明

instance-id	スパニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ～ 4094 です。
priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、スイッチがルート スイッチとして選択される可能性に影響します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ～ 61440 であり、刻み幅は 4096 です。有効なプライオリティ値は 0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。それ以外の値はすべて拒否されます。

デフォルト

デフォルト値は 32768 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

例

次の例では、Multiple Spanning-Tree（MST）インスタンス 20 ～ 21 のスパニングツリー プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

設定を確認するには、**show spanning-tree mst** *instance-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	特定のインターフェイスの MST 情報を表示します。
spanning-tree mst cost	MST の計算に使用するパス コストを設定します。
spanning-tree mst port-priority	インターフェイス プライオリティを設定します。

spanning-tree mst root

ネットワークの直径に基づいて Multiple Spanning-Tree（MST）ルート スイッチのプライオリティとタイマーを設定するには、**spanning-tree mst root** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

シンタックスの説明

instance-id	スパニングツリー インスタンス範囲。1 つのインスタンス、それぞれをハイフンで区切ったインスタンスの範囲、またはカンマで区切った一連のインスタンスを指定することができます。指定できる範囲は 0 ～ 4094 です。
root primary	このスイッチを強制的にルート スイッチに設定します。
root secondary	プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter *net-diameter*	（任意）2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ～ 7 です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。
hello-time *seconds*	（任意）ルート スイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔を設定します。指定できる範囲は 1 ～ 10 秒です。このキーワードは、MST インスタンス 0 の場合のみ使用できます。

デフォルト

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 です。

hello タイムは 2 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SED	*instance-id* の範囲が 1 ～ 4094 に変更されました。

使用上のガイドライン

spanning-tree mst *instance-id* **root** コマンドは、バックボーン スイッチでのみ使用してください。

spanning-tree mst *instance-id* **root** コマンドを入力すると、ソフトウェアはこのスイッチをスパニングツリー インスタンスのルートに設定するのに十分なプライオリティを設定しようとします。拡張システム ID がサポートされているため、スイッチはインスタンスのスイッチ プライオリティを 24576 に設定します（この値によってこのスイッチが指定されたインスタンスのルートになる場合）。指定インスタンスのルート スイッチに、24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチ プライオリティより 4096 小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。

spanning-tree mst *instance-id* **root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアによりスイッチ プライオリティがデフォルト値（32768）から 28672 に変更されます。ルート スイッチに障害が発生した場合は、このスイッチが次のルート スイッチになります（ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティ 32768 を使用しているためにルート スイッチになる可能性が低い場合）。

例

次の例では、スイッチをインスタンス 10 のルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

次の例では、スイッチをインスタンス 10 のセカンダリ ルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree mst** *instance-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst *instance-id*	指定インスタンスの MST 情報を表示します。
spanning-tree mst forward-time	すべての MST インスタンスについて転送遅延時間を設定します。
spanning-tree mst hello-time	ルート スイッチ コンフィギュレーション メッセージが送信する hello BPDU の間隔を設定します。
spanning-tree mst max-age	スパニング ツリーがルート スイッチからメッセージを受信する間隔を指定します。
spanning-tree mst max-hops	BPDU がドロップされるまでのリージョンのホップ数を設定します。

spanning-tree port-priority

インターフェイス プライオリティを設定するには、**spanning-tree port-priority** インターフェイス コンフィギュレーション コマンドを使用します。ループが発生した場合、スパニング ツリーはフォワーディング ステートにするインターフェイスを判別できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree [**vlan** *vlan-id*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

シンタックスの説明

vlan *vlan-id*	（任意）スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ～ 4094 です。
priority	使用できる番号は 0 ～ 240 で、16 ずつ増加します。有効なプライオリティ値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、および 240 です。それ以外の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。

デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

変数 *vlan-id* を省略した場合、このコマンドは VLAN 1 に関連付けられたスパニングツリー インスタンスに適用されます。

インターフェイスが割り当てられていない VLAN にも、プライオリティを設定できます。このインターフェイスを VLAN に割り当てると、設定が有効になります。

インターフェイスを **spanning-tree vlan** *vlan-id* **port-priority** *priority* コマンドおよび **spanning-tree port-priority** *priority* コマンドを両方使用して設定する場合、**spanning-tree vlan** *vlan-id* **port-priority** *priority* コマンドが有効になります。

例

次の例では、ループが発生した場合にポートがフォワーディング ステートになる可能性を高める方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

次の例では、VLAN 20 ～ 25 のポート プライオリティ値を設定する方法を示します。

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

設定を確認するには、**show spanning-tree interface** *interface-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree interface *interface-id*	特定のインターフェイスのスパニングツリー情報を表示します。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree vlan priority	指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。

spanning-tree portfast（グローバル コンフィギュレーション）

PortFast 対応のインターフェイス上で BPDU フィルタリングおよび BPDU ガード機能をグローバルにイネーブルにしたり、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにしたりするには、**spanning-tree portfast** グローバル コンフィギュレーション コマンドを使用します。BPDU フィルタリング機能を使用すると、スイッチ インターフェイスでの BPDU の送受信を禁止できます。BPDU ガード機能は、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

シンタックスの説明

bpdufilter default	PortFast 対応インターフェイス上で BPDU フィルタリングをグローバルにイネーブルにし、エンド ステーションに接続されたスイッチ インターフェイスでの BPDU の送受信を禁止します。
bpduguard default	PortFast 対応インターフェイス上で BPDU ガード機能をグローバルにイネーブルにし、BPDU を受信する PortFast 対応インターフェイスを errdisable ステートにします。
default	すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。

デフォルト

BPDU フィルタリング、BPDU ガード、および PortFast 機能は、個別に設定しないかぎり、すべてのインターフェイスでディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、これらの機能をイネーブルにできます。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドは、PortFast 対応インターフェイス（PortFast 動作ステートのインターフェイス）上で BPDU フィルタリングをグローバルにイネーブルにします。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。スイッチ インターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU を受信した PortFast 対応インターフェイスでは PortFast 動作ステータスが解除され、BPDU フィルタリングがディセーブルになります。

spanning-tree portfast bpdufilter default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpufilter** インターフェイス コンフィギュレーション コマンドを使用します。

注意　BPDU フィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリー ループが発生することがあります。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドは、PortFast 動作ステートのインターフェイス上で BPDU ガードをグローバルにイネーブルにします。有効な設定では、PortFast 対応インターフェイスは BPDU を受信しません。PortFast 対応インターフェイスが BPDU を受信した場合は、認可されていない装置の接続などのような無効な設定が存在することを示しており、BPDU ガード機能によってインターフェイスは errdisable ステートになります。インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニング ツリーに参加しないようにするには、BPDU ガード機能を使用します。

spanning-tree portfast bpduguard default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree bdpuguard** インターフェイス コンフィギュレーション コマンドを使用します。

すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにするには、**spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用します。PortFast は、エンド ステーションに接続するインターフェイスに限って設定します。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。リンクがアップすると、PortFast 対応インターフェイスは標準の転送遅延時間の経過を待たずに、ただちにスパニングツリーフォワーディング ステートに移行します。

spanning-tree portfast default グローバル コンフィギュレーション コマンドの設定を上書きするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用します。**no spanning-tree portfast default** グローバル コンフィギュレーション コマンドを使用すると、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用してポートを個別に設定した場合を除き、すべてのインターフェイス上で PortFast をディセーブルにすることができます。

例

次の例では、BPDU フィルタリング機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpdufilter default
```

次の例では、BPDU ガード機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast bpduguard default
```

次の例では、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにする方法を示します。

```
Switch(config)# spanning-tree portfast default
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree bpdufilter	インターフェイスが BPDU を送受信しないようにします。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。

spanning-tree portfast（インターフェイス コンフィギュレーション）

対応するすべての VLAN 内の特定のインターフェイス上で PortFast 機能をイネーブルにするには、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用します。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

シンタックスの説明

disable	（任意）指定されたインターフェイスの PortFast 機能をディセーブルにします。
trunk	（任意）トランキング インターフェイスの PortFast 機能をイネーブルにします。

デフォルト

すべてのインターフェイスで PortFast 機能はディセーブルですが、ダイナミック アクセス ポートでは自動的にイネーブルになります。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

この機能は、エンド ステーションに接続するインターフェイスに限って使用します。そうしないと、偶発的なトポロジ ループが原因でパケット ループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

トランク ポートで PortFast をイネーブルにするには、**spanning-tree portfast trunk** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**spanning-tree portfast** コマンドは、トランク ポートではサポートされません。

スイッチが Per-VLAN Spanning-Tree Plus（PVST+）モード、Rapid PVST+ モード、または Multiple Spanning-Tree（MST）モードで稼動している場合は、その機能をイネーブルにできます。

この機能はインターフェイス上のすべての VLAN に影響します。

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、ただちにスパニングツリー フォワーディング ステートに移行されます。

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランク インターフェイス上で PortFast 機能をグローバルにイネーブルにできます。ただし、**spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して、グローバル設定を上書きできます。

spanning-tree portfast default グローバル コンフィギュレーション コマンドを設定する場合は、**spanning-tree portfast disable** インターフェイス コンフィギュレーション コマンドを使用して、トランク インターフェイス以外のインターフェイス上で PortFast 機能をイネーブルにできます。

例

次の例では、特定のポート上で PortFast 機能をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
spanning-tree bpdufilter	インターフェイスでのブリッジ プロトコル データ ユニット（BPDU）の送受信を禁止します。
spanning-tree bpduguard	BPDU を受信したインターフェイスを、errdisable ステートにします。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。

spanning-tree transmit hold-count

毎秒送信するブリッジ プロトコル データ ユニット（BPDU）の数を設定するには、**spanning-tree transmit hold-count** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree transmit hold-count [*value*]

no spanning-tree transmit hold-count [*value*]

シンタックスの説明

value	（任意）毎秒送信される BPDU 数。指定できる範囲は 1 ～ 20 です。

デフォルト

デフォルト値は 6 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)SED	このコマンドが追加されました。

使用上のガイドライン

スイッチが Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）モードの場合、伝送ホールド カウント値が増加すると、CPU の使用率に大きく影響する可能性があります。この値を減らすと、コンバージェンスの速度が低下します。デフォルト設定を使用することを推奨します。

例

次の例では、伝送ホールド カウントを 8 に設定する方法を示します。

```
Switch(config)# spanning-tree transmit hold-count 8
```

設定を確認するには、**show spanning-tree mst** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree mst	伝送ホールド カウントを含む、Multiple Spanning-Tree（MST）のリージョン設定およびステータスを表示します。

spanning-tree uplinkfast

リンクやスイッチに障害が発生した場合またはスパニングツリーが自動的に再設定された場合に新しいルート ポートを短時間で選択できるようにするには、**spanning-tree uplinkfast** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree uplinkfast [**max-update-rate** *pkts-per-second*]

no spanning-tree uplinkfast [**max-update-rate**]

シンタックスの説明

max-update-rate *pkts-per-second*	（任意）更新パケットを送信するときの 1 秒間のパケット数です。指定できる範囲は 0 ～ 32000 です。

デフォルト

UplinkFast はディセーブルです。

更新速度は 150 パケット / 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、アクセス スイッチ上だけで使用します。

UplinkFast 機能は、Rapid PVST+ または Multiple Spanning-Tree（MST）モード用に設定できますが、スパニングツリー モードを PVST+ に変更するまでこの機能はディセーブル（非アクティブ）のままです。

UplinkFast をイネーブルにすると、スイッチ全体に対してイネーブルになり、VLAN 単位でイネーブルにすることはできません。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチ プライオリティが 49152 に設定されます。UplinkFast をイネーブルにした場合または UplinkFast がすでにイネーブルになっている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスと VLAN トランクのパス コストが 3000 だけ増加します（パス コストを 3000 以上の値に変更した場合、パス コストは変更されません）。スイッチ プライオリティおよびパス コストを変更すると、スイッチがルート スイッチになる可能性が低下します。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチ プライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

ルート ポートに障害が発生していることがスパニング ツリーで検出されると、UplinkFast はスイッチをただちに代替ルート ポートに変更して、新しいルート ポートを直接フォワーディング ステートに移行させます。この間、トポロジ変更通知が送信されます。

UplinkFast 機能が使用するインターフェイスで、ルート ガードをイネーブルにしないでください。UplinkFast を使用すると、障害発生時に（ブロッキング ステートの）バックアップ インターフェイスがルート ポートになります。しかし、同時にルート ガードもイネーブルになっていた場合は、UplinkFast 機能が使用するすべてのバックアップ インターフェイスが root-inconsistent（ブロック）になり、フォワーディング ステートに移行できなくなります。

max-update-rate を 0 に設定すると、ステーションを学習するフレームが生成されず、接続の切断後、スパニングツリー トポロジのコンバージェンスに要する時間が長くなります。

例

次の例では、UplinkFast をイネーブルにする方法を示します。

```
Switch(config)# spanning-tree uplinkfast
```

設定を確認するには、**show spanning-tree summary** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree summary	スパニングツリー インターフェイス ステートのサマリーを表示します。
spanning-tree vlan root primary	このスイッチを強制的にルート スイッチに設定します。

spanning-tree vlan

VLAN 単位でスパニングツリーを設定するには、**spanning-tree vlan** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

シンタックスの説明

vlan-id	スパニングツリー インスタンスに関連付けられた VLAN 範囲です。VLAN ID 番号で識別された 1 つの VLAN、それぞれをハイフンで区切った VLAN 範囲、またはカンマで区切った一連の VLAN を指定することができます。指定できる範囲は 1 ～ 4094 です。
forward-time *seconds*	（任意）指定したスパニングツリー インスタンスの転送遅延時間を設定します。転送遅延時間には、インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートが継続する時間を指定します。指定できる範囲は 4 ～ 30 秒です。
hello-time *seconds*	（任意）ルート スイッチ コンフィギュレーション メッセージで送信される hello BPDU の間隔を設定します。指定できる範囲は 1 ～ 10 秒です。
max-age *seconds*	（任意）スパニング ツリーがルート スイッチからメッセージを受信する間隔を設定します。スイッチがこのインターバル内にルート スイッチから BPDU メッセージを受信しない場合は、スパニングツリー トポロジが再計算されます。指定できる範囲は 6 ～ 40 秒です。
priority *priority*	（任意）指定したスパニングツリー インスタンスのスイッチ プライオリティを設定します。この設定は、このスイッチがルート スイッチとして選択される可能性に影響します。小さい値を設定すると、スイッチがルート スイッチとして選択される可能性が高まります。 指定できる範囲は 0 ～ 61440 であり、刻み幅は 4096 です。有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、および 61440 です。それ以外の値はすべて拒否されます。
root primary	（任意）このスイッチを強制的にルート スイッチに設定します。
root secondary	（任意）プライマリ ルート スイッチに障害が発生した場合に、このスイッチをルート スイッチに設定します。
diameter *net-diameter*	（任意）2 つのエンド ステーション間にスイッチの最大数を設定します。指定できる範囲は 2 ～ 7 です。

デフォルト

すべての VLAN でスパニング ツリーがイネーブルです。

転送遅延時間は 15 秒です。

hello タイムは 2 秒です。

有効期限は 20 秒です。

プライマリ ルート スイッチのプライオリティは 24576 です。

セカンダリ ルート スイッチのプライオリティは 28672 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

STP をディセーブルにすると、VLAN はスパニングツリー トポロジへの参加を停止します。管理上のダウン状態のインターフェイスは、ダウン状態のままです。受信された BPDU は、他のマルチキャスト フレームと同様に転送されます。STP がディセーブルの場合、VLAN はループの検出や禁止を行いません。

現在アクティブではない VLAN 上で STP をディセーブルにしたり、変更を確認するには、**show running-config** または **show spanning-tree vlan** *vlan-id* 特権 EXEC コマンドを使用します。設定は、VLAN がアクティブである場合に有効となります。

STP をディセーブルにするか、再びイネーブルにすると、ディセーブルまたはイネーブルにする VLAN 範囲を指定できます。

VLAN をディセーブルにしてからイネーブルにした場合、その VLAN に割り当てられていたすべての VLAN は引き続きメンバーとなります。ただし、すべてのスパニングツリー ブリッジ パラメータは元の設定（VLAN がディセーブルになる直前の設定）に戻ります。

インターフェイスが割り当てられていない VLAN 上で、スパニングツリー オプションをイネーブルにすることができます。インターフェイスに設定を割り当てると、設定が有効になります。

max-age *seconds* を設定すると、指定されたインターバル内にスイッチがルート スイッチから BPDU を受信しなかった場合に、スパニングツリー トポロジが再計算されます。**max-age** の設定値は、**hello-time** の設定値よりも大きくなければなりません。

spanning-tree vlan *vlan-id* **root** コマンドは、バックボーン スイッチでのみ使用してください。

spanning-tree vlan *vlan-id* **root** コマンドを入力すると、ソフトウェアは各 VLAN の現在のルート スイッチのスイッチ プライオリティを確認します。拡張システム ID がサポートされているため、スイッチは指定された VLAN のスイッチ プライオリティを 24576 に設定します。これは、この値によってこのスイッチが指定された VLAN のルートになる場合です。指定された VLAN のルート スイッチに 24576 に満たないスイッチ プライオリティが設定されている場合は、スイッチはその VLAN について、自身のプライオリティを最小のスイッチ プライオリティより 4096 だけ小さい値に設定します（4096 は 4 ビット スイッチ プライオリティの最下位ビットの値です）。

spanning-tree vlan *vlan-id* **root secondary** コマンドを入力すると、拡張システム ID がサポートされているため、ソフトウェアによりスイッチ プライオリティがデフォルト値（32768）から 28672 に変更されます。ルート スイッチに障害が発生した場合は、このスイッチが次のルート スイッチになります（ネットワーク内の他のスイッチがデフォルトのスイッチ プライオリティ 32768 を使用しているためにルート スイッチになる可能性が低い場合）。

例

次の例では、VLAN 5 上で STP をディセーブルにする方法を示します。

```
Switch(config)# no spanning-tree vlan 5
```

設定を確認するには、**show spanning-tree** 特権 EXEC コマンドを入力します。このインスタンスのリストに、VLAN 5 は表示されません。

次の例では、VLAN 20 と VLAN 25 のスパニングツリーについて、転送時間を 18 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

次の例では、VLAN 20 ～ 24 のスパニングツリーについて、hello 遅延時間を 3 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

次の例では、VLAN 20 のスパニングツリーについて、有効期限を 30 秒に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

次の例では、スパニングツリー インスタンス 100 およびインスタンス 105 ～ 108 の **max-age** パラメータをデフォルト値に戻す方法を示します。

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

次の例では、VLAN 20 のスパニングツリーについて、プライオリティを 8192 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

次の例では、スイッチを VLAN 10 のルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

次の例では、スイッチを VLAN 10 のセカンダリ ルート スイッチとして設定し、ネットワーク直径を 4 に設定する方法を示します。

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

設定を確認するには、**show spanning-tree vlan** *vlan-id* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show spanning-tree vlan	スパニングツリー情報を表示します。
spanning-tree cost	スパニングツリーの計算に使用するパス コストを設定します。
spanning-tree guard	選択されたインターフェイスに対応するすべての VLAN に対して、ルート ガード機能またはループ ガード機能をイネーブルにします。
spanning-tree port-priority	インターフェイス プライオリティを設定します。
spanning-tree portfast（グローバル コンフィギュレーション）	PortFast 対応インターフェイス上で BPDU フィルタリング機能または BPDU ガード機能をグローバルにイネーブルにするか、またはすべての非トランク インターフェイスで PortFast 機能をイネーブルにします。
spanning-tree portfast（インターフェイス コンフィギュレーション）	対応するすべての VLAN 内の特定のインターフェイスで、PortFast 機能をイネーブルにします。
spanning-tree uplinkfast	UplinkFast 機能をイネーブルにし、新しいルート ポートを短時間で選択できるようにします。

speed

10/100 Mb/s ポートまたは 10/100/1000 Mb/s ポートの速度を指定するには、**speed** インターフェイス コンフィギュレーション コマンドを使用します。ポートをデフォルト値に戻すには、このコマンドの **no** または **default** 形式を使用します。

speed {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

no speed

シンタックスの説明

10	ポートは 10 Mb/s で稼動します。
100	ポートは 100 Mb/s で稼動します。
1000	ポートは 1000 Mb/s で稼動します。このオプションは、10/100/1000 Mb/s ポートでのみ有効であり、これらのポート上にのみ表示されます。
auto	ポートが自動的に、もう一方のリンクの終端ポートを基準にして速度を検出します。**10**、**100**、または **1000** キーワードと **auto** キーワードを一緒に使用する場合、ポートは指定した速度で自動ネゴシエーションだけを行います。
nonegotiate	自動ネゴシエーションがディセーブルになり、ポートが 1000 Mb/s で稼動します（1000BASE-T SFP は nonegotiate キーワードをサポートしていません）。

デフォルト

デフォルトの設定は **auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

自動ネゴシエーションをサポートしていないデバイスに SFP モジュール ポートが接続されている場合は、ネゴシエートしないように（**nonegotiate**）速度を設定できます。

速度が **auto** に設定されている場合、スイッチはリンクの反対側のデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

ラインの両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。インターフェイス 1 つが自動ネゴシエーションをサポートし、相手側がサポートしない場合、サポート側は **auto** 設定を使用しますが、相手側にデュプレックスおよび速度を設定します。

注意　インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再度イネーブルになる場合があります。

スイッチの速度パラメータとデュプレックス パラメータの設定に関する注意事項については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

例

次の例では、ポートの速度を 100 Mbps に設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

次の例では、10 Mb/s でだけポートが自動ネゴシエートするように設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

次の例では、10 Mb/s または 100 Mb/s でだけポートが自動ネゴシエートするように設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
duplex	デュプレックス モードの動作を指定します。
show interfaces	すべてのインターフェイスまたは特定のインターフェイスに対する統計情報を表示します。

srr-queue bandwidth limit

ポートの最大出力を制限するには、**srr-queue bandwidth limit** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

srr-queue bandwidth limit *weight1*

no srr-queue bandwidth limit

（注）　このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

weight1	制限されるポート速度のパーセント。指定できる範囲は 10 ～ 90 です。

デフォルト

ポートはレート制限されておらず、100% に設定されます。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ライン レートは接続速度の 80% に下がります。ただし、ハードウェアはライン レートが 6 つずつ増加するよう調整しているので、この値は厳密ではありません。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、これらの設定がユーザの QoS（Quality of Service）ソリューションを満たさないと判断した場合のみ、設定を変更することができます。

例

次の例では、ポートを 800 Mb/s に制限する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos srr-queue output cos-map	サービス クラス（CoS）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface queueing	QoS 情報を表示します。
srr-queue bandwidth shape	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。
srr-queue bandwidth share	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

srr-queue bandwidth shape

シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅のシェーピングをイネーブルにするには、**srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

srr-queue bandwidth shape *weight1 weight2 weight3 weight4*

no srr-queue bandwidth shape

（注）　このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

weight1 weight2 weight3 weight4	シェーピングされるポートのパーセントを判別する重みを指定します。インバース比（1/*weight*）は、このキューのシェーピング帯域幅を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 65535 です。

デフォルト

ウェイト 1 は 25 に設定されています。ウェイト 2、ウェイト 3、および ウェイト 4 は 0 に設定されており、これらのキューは共有モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

シェーピング モードでは、キューは帯域幅のパーセントとして保証され、この量にレート制限されます。リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を越えて使用できません。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。

シェーピング モードは、共有モードを無効にします。

srr-queue bandwidth shape インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは共有モードに参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューにシェーピングと共有を混在させて設定する場合、最小のキューをシェーピングに設定します。

（注）　出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

例

次の例では、同じポートのキューをシェーピングと共有両方に設定する方法を示します。キュー 2、3、4 の重み比が 0 に設定されているので、キューは共有モードで動作します。キューの帯域幅の重みは 1/8、12.5% です。キュー 1 は、この帯域幅で保証され制限されています。他のキューにトラフィックがなくアイドルであっても、他のキューにスロットを拡張しません。キュー 2、3、4 は共有モードで、キュー 1 の設定は無視されます。共有モードのキューに割り当てられた帯域幅比は、4/（4+4+4）、33% です。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
Switch(config-if)# srr-queue bandwidth share 4 4 4 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	サービス クラス（CoS）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface queueing	QoS（Quality of Service）情報を表示します。
srr-queue bandwidth share	共有ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅の共有をイネーブルにします。

srr-queue bandwidth share

シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにするには、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。重み比は、Shaped Round Robin（SRR）スケジューラが各キューからパケットを取り出す周波数比です。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

srr-queue bandwidth share *weight1 weight2 weight3 weight4*

no srr-queue bandwidth share

（注）このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

weight1 weight2 weight3 weight4	*weight1*、*weight2*、*weight3*、および *weight4* は、SRR スケジューラがパケットを取り出す周波数比を指定します。各値はスペースで区切ります。指定できる範囲は 1 ～ 255 です。

デフォルト

ウェイト 1、ウェイト 2、ウェイト 3 およびウェイト 4 は 25 に設定されています（各キューに帯域幅の 1/4 を割り当て）。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

各重みの絶対値は意味がないので、パラメータ比だけを使用します。

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。

srr-queue bandwidth shape インターフェイス コンフィギュレーション コマンドを使用してシェーピングされたキューの重みを 0 に設定すると、このキューは SRR 共有モードに参加します。**srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。

同じポートのキューにシェーピングと共有を混在させて設定する場合、最小のキューをシェーピングに設定します。

（注）出力キューのデフォルト設定は、ほとんどの状況に適しています。出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合のみ、設定を変更してください。

例

次の例では、出力ポートで稼動する SRR スケジューラの重みの比を設定する方法を示します。キュー 4 つを使用します。共有モードの各キューに割り当てられた帯域幅は 1/（1+2+3+4）、2/（1+2+3+4）、3/（1+2+3+4）、および 4/（1+2+3+4）であり、キュー 1、2、3、および 4 に対してそれぞれ 10%、20%、30%、および 40% です。つまり、キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍になります。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

設定を確認するには、**show mls qos interface** [*interface-id*] **queueing** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	キューセットに対しバッファを割り当てます。
mls qos srr-queue output cos-map	サービス クラス（CoS）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos srr-queue output dscp-map	Differentiated Service Code Point（DSCP）値を出力キュー、またはキューとしきい値 ID にマッピングします。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キューセットに対する最大メモリ割り当てを設定します。
priority-queue	ポート上で出力緊急キューをイネーブルにします。
queue-set	キューセットに対しポートをマッピングします。
show mls qos interface queueing	QoS（Quality of Service）情報を表示します。
srr-queue bandwidth shape	シェーピング ウェイトを割り当て、ポートにマッピングされた 4 つの出力キュー上の帯域幅のシェーピングをイネーブルにします。

storm-control

インターフェイス上でブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御をイネーブルにし、しきい値のレベルを設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

storm-control {{**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

no storm-control {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

シンタックスの説明

broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。
unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level *level* [*level-low*]	上限および下限抑制レベルをポートの全帯域幅のパーセンテージとして指定します。 • *level*：上限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。指定した *level* の値に達した場合、ストーム パケットのフラッディングをブロックします。 • *level-low*：（任意）下限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。この値は、上限抑制値より小さいまたは等しい必要があります。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。
level bps *bps* [*bps-low*]	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（ビット / 秒）として指定します。 • *bps*：上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した *bps* の値に達した場合、ストーム パケットのフラッディングをブロックします。 • *bps-low*：（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は、上限抑制値に等しいまたは小さい必要があります。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。

level pps *pps* [*pps-low*]	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（パケット/秒）として指定します。 • *pps*：上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した *pps* の値に達した場合、ストーム パケットのフラッディングをブロックします。 • *pps-low*：（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は、上限抑制値に等しいまたは小さい必要があります。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
action {**shutdown** | **trap**}	ポートでストームが発生した場合にとられるアクション。デフォルト アクションは、トラフィックをフィルタし、SNMP（簡易ネットワーク管理プロトコル）トラップを送信しません。 キーワードの意味は次のとおりです。 • **shutdown**：ストームの間、ポートをディセーブルにします。 • **trap**：ストーム発生時に、SNMP トラップを送信します。

デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。

デフォルト アクションは、トラフィックをフィルタし、SNMP トラップを送信しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ストーム制御抑制レベルは、ポートの全帯域幅のパーセンテージとして、トラフィックが受信される速度（1 秒あたりのパケット数、または 1 秒あたりのビット数）として入力できます。

全帯域幅のパーセンテージとして指定した場合、100% の抑制値は、指定したトラフィック タイプに制限が設定されていないことを意味します。**level 0 0** の値は、ポート上のすべてのブロードキャスト、マルチキャスト、ユニキャスト トラフィックをブロックします。ストーム制御は、上限抑制レベルが 100% 未満の場合のみイネーブルになります。他のストーム制御設定が指定されていない場合、デフォルト アクションは、ストームの原因となっているトラフィックをフィルタし、SNMP トラップを送信しません。

（注）マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどのコントロール トラフィック以外のマルチキャスト トラフィックすべてがブロックされます。

trap および **shutdown** オプションは、互いに独立しています。

パケット ストームが検出されたときにシャットダウンを行う（ストームの間、ポートが errdisable になる）ようにアクションを設定する場合、インターフェイスをこのステートから解除するには **no shutdown** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**shutdown** アクションを指定しない場合、**trap**（ストーム検出時にスイッチがトラップを生成する）として指定してください。

ストームが発生し、実行されるアクションがトラフィックのフィルタリングである場合、下限抑制レベルが指定されていないと、トラフィック レートが上限抑制レベルより低くなるまでスイッチはすべてのトラフィックをブロックします。下限抑制レベルが指定されている場合、トラフィック レートがこのレベルより低くなるまでスイッチはトラフィックをブロックします。

（注）　ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ブロードキャスト ストームが発生し、実行されるアクションがトラフィックのフィルタである場合、スイッチはブロードキャスト トラフィックのみをブロックします。

詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、75.5% の上限抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例では、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例では、2000 パケット / 秒の上限抑制レベルと 1000 パケット / 秒の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、ポートで **shutdown** アクションをイネーブルにする方法を示します。

```
Switch(config-if)# storm-control action shutdown
```

設定を確認するには、**show storm-control** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show storm-control	すべてのインターフェイス上、または指定のインターフェイス上で、ブロードキャスト、マルチキャストまたはユニキャスト ストーム制御の設定を表示します。

switchport access

ポートをスタティックアクセス ポートまたはダイナミックアクセス ポートとして設定するには、**switchport access** インターフェイス コンフィギュレーション コマンドを使用します。スイッチポートのモードが、**access** に設定されている場合、ポートは指定の VLAN のメンバーとして動作します。**dynamic** として設定されている場合、ポートは受信した着信パケットに基づいて、VLAN 割り当ての検出を開始します。アクセス モードをスイッチのデフォルト VLAN にリセットするには、このコマンドの **no** 形式を使用します。

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

シンタックスの説明

vlan *vlan-id*	インターフェイスを、アクセス モード VLAN の VLAN ID を持つスタティック アクセス ポートとして設定します。指定できる範囲は 1 ～ 4094 です。
vlan dynamic	VLAN メンバシップ ポリシー サーバ（VMPS）プロトコルによってアクセス モード VLAN が決まるように指定します。ポートに接続されたホスト（複数可）の送信元 MAC（メディア アクセス制御）アドレスに基づいて、ポートが VLAN に割り当てられます。スイッチは受信された新しい MAC アドレスをすべて VMPS サーバに送信して、ダイナミック アクセス ポートに割り当てる VLAN の名前を取得します。ポートにすでに VLAN が割り当てられていて、送信元が VMPS によって承認されている場合、スイッチはパケットを該当する VLAN に転送します。

デフォルト

デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

ダイナミック アクセス ポートは最初はどの VLAN にも属さず、受信したパケットに基づいて割り当てを受信します。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

no switchport access コマンドを使用すると、アクセス モード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

switchport access vlan コマンドを有効にするには、ポートをアクセス モードにする必要があります。

アクセス ポートを割り当てることができるのは、1 つの VLAN のみです。

ポートをダイナミックとして設定するには、事前に VMPS サーバ（Catalyst 6000 シリーズ スイッチなど）を設定する必要があります。

ダイナミック アクセス ポートには、次の制限事項が適用されます。

- ソフトウェアでは、Catalyst 6000 シリーズ スイッチなどの VMPS をクエリーできる VLAN Query Protocol（VQP）クライアントが実装されます。Catalyst 2960 スイッチは、VMPS サーバではありません。ポートをダイナミックとして設定するには、事前に VMPS サーバを設定する必要があります。
- ダイナミック アクセス ポートは、エンド ステーションを接続する場合のみ使用します。ブリッジング プロトコルを使用するスイッチまたはルータにダイナミック アクセス ポートを接続すると、接続が切断されることがあります。
- スパニングツリー プロトコル（STP）がダイナミック アクセス ポートを STP ブロッキング ステートにしないように、ネットワークを設定します。ダイナミック アクセス ポートでは、PortFast 機能が自動的にイネーブルになります。
- ダイナミック アクセス ポートは、1 つの VLAN にのみ属することができ、VLAN タギングは使用しません。
- ダイナミック アクセス ポートを次のように設定することはできません。
  - EtherChannel ポート グループのメンバー（ダイナミック アクセス ポートは、他のダイナミック ポートを含めて、他のポートとグループ化できません）
  - スタティック アドレス エントリ内の送信元または宛先ポート
  - モニタ ポート

例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスがデフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
Switch(config-if)# switchport access vlan 2
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力して、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport mode	ポートの VLAN メンバシップ モードを設定します。

switchport backup interface

1 組のインターフェイスで相互にバックアップを提供する Flex Link を設定するには、レイヤ 2 インターフェイス上で **switchport backup interface** インターフェイス コンフィギュレーション コマンドを使用します。Flex Link 設定を削除するには、このコマンドの **no** 形式を使用します。

switchport backup interface [**FastEthernet** *interface-id* | **GigabitEthernet** *interface-id* | **Port-channel** *interface-id* | **TenGigabitEthernet** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

no switchport backup interface [**FastEthernet** *interface-id* | **GigabitEthernet** *interface-id* | **Port-channel** *interface-id* | **TenGigabitEthernet** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

（注）　このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

FastEthernet	ファスト イーサネット IEEE 802.3 ポート名。指定できる範囲は 0 ～ 9 です。
GigabitEthernet	ギガビット イーサネット IEEE 802.3z ポート名。指定できる範囲は 0 ～ 9 です。
Port-channel	インターフェイスのイーサネット チャネル。指定できる範囲は 0 ～ 48 です。
TenGigabitEthernet	10 ギガビット イーサネット ポート名。指定できる範囲は 0 ～ 9 です。
interface-id	設定されるインターフェイスへのバックアップ リンクとしてレイヤ 2 インターフェイスが機能するように指定します。このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 486 です。
mmu	MAC アドレス移行更新。バックアップ インターフェイス ペアの Mac Move Update（MMU）を設定します。
primary vlan *vlan-id*	プライマリ VLAN となるプライベート VLAN の VLAN ID。指定できる範囲は 1 ～ 4,094 です。
multicast fast-convergence	マルチキャスト ファストコンバージェンス パラメータ。
preemption	バックアップ インターフェイス ペアのプリエンプション スキームを設定します。
delay *delay-time*	（任意）プリエンプション遅延を指定します。指定できる範囲は、1 ～ 300 秒です。
mode	プリエンプション モードを bandwidth、forced、または off に設定します。
prefer vlan *vlan-id*	VLAN が Flex Link ペアのバックアップ インターフェイスで実行されるように指定します。VLAN ID 範囲は 1 ～ 4,094 です。
off	（任意）バックアップからアクティブへ移行する際、プリエンプションを行わないように指定します。
delay *delay-time*	（任意）プリエンプション遅延を指定します。指定できる範囲は、1 ～ 300 秒です。

デフォルト

デフォルトは、Flex Link が定義されていません。プリエンプション モードはオフです。プリエンプションを行いません。プリエンプション遅延は 35 秒に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(25)SEE	**preemption**、**mode**、**forced**、**bandwidth**、**off**、および **delay** キーワードが追加されました。
12.2(37)SE	**prefer vlan** キーワードが追加されました。
12.2(44)SE	**multicast**、**fast-convergence**、**delay**、**mode**、**prefer**、および **vlan** キーワードが追加されました。

使用上のガイドライン

Flex Link を設定すると、1 つのリンクがプライマリ インターフェイスとして機能してトラフィックを転送し、もう一方のインターフェイスがスタンバイ モードになり、プライマリ リンクがシャットダウンされた場合に転送を開始できるように準備されます。設定されるインターフェイスはアクティブ リンクと呼ばれ、指定されたインターフェイスをバックアップ リンクとして識別されます。この機能はスパニングツリー プロトコル（STP）の代わりに提供され、ユーザが STP をオフにした場合でも基本的なリンク冗長性を維持できます。

- このコマンドは、レイヤ 2 インターフェイスに対してのみ使用可能です。
- アクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。
- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つのアクティブ リンクに対してのみバックアップ リンクになれます。アクティブ リンクは別の FLex Link ペアに属することはできません。
- バックアップ リンクはアクティブ リンクと同じタイプ（たとえばファスト イーサネットやギガビット イーサネット）でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の FLex Link を似たような特性で設定する必要があります。
- いずれのリンクも EtherChannel に属するポートにはなれません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルと物理インターフェイスを Flex Link として設定でき、ポート チャネルまたは物理インターフェイスをアクティブ リンクにできます。
- STP がスイッチに設定されている場合、Flex Link はすべての有効な VLAN で STP に参加しません。STP が動作していない場合、設定されているトポロジでループが発生していないことを確認してください。

例

次に、2 つのインターフェイスを Flex Link として設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end
```

次の例では、常にバックアップをプリエンプトするようにファスト イーサネット インターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preemption forced
Switch(conf-if)# end
```

次の例では、ファスト イーサネット インターフェイスのプリエンプション遅延時間を設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 preemption delay 150
Switch(conf-if)# end
```

次の例では、MMU プライマリ VLAN としてファスト イーサネット インターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# switchport backup interface fastethernet0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

設定を確認するには、show interfaces switchport backup 特権 EXEC コマンドを入力します。

次の例では、優先 VLAN を設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/6
Switch(config-if)# switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120
```

設定を確認するには、**show interfaces switchport backup** 特権 EXEC コマンドを入力します。

この例では、VLAN 60、および 100 ～ 120 がスイッチに設定されています。

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi0/6 が VLAN 1 ～ 50 のトラフィックを転送し、Gi0/8 が VLAN 60 および 100 ～ 120 のトラフィックを転送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6 GigabitEthernet0/8 Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi0/6 がダウンすると、Gi0/8 が Flex Link ペアのすべての VLAN を伝送します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6 GigabitEthernet0/8 Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi0/6 がアップになって、このインターフェイスに指定されていた VLAN がピア インターフェイス Gi0/8 上でブロックされ、Gi0/6 に転送されます。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6 GigabitEthernet0/8 Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

次の例では、インターフェイス Gi0/11 上でマルチキャスト ファストコンバージェンスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 0/12 multicast
fast-convergence
Switch(config-if)# end
```

設定を確認するには、**show interfaces switchport backup detail** 特権 EXEC コマンドを入力します。

```
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : On
        Bandwidth : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)
        Mac Address Move Update Vlan : auto
```

関連コマンド

コマンド	説明
show interfaces [*interface-id*] **switchport backup**	スイッチまたは指定されているインターフェイスに設定されている Flex Link とそのステータスを表示します。

switchport block

不明なマルチキャストまたはユニキャストのパケットが転送されないようにするには、**switchport block** インターフェイス コンフィギュレーション コマンドを使用します。未知のマルチキャストまたはユニキャスト パケットの転送を許可するには、このコマンドの **no** 形式を使用します。

switchport block {**multicast** | **unicast**}

no switchport block {**multicast** | **unicast**}

シンタックスの説明

multicast	不明なマルチキャスト トラフィックをブロックするよう指定します。
unicast	不明なユニキャスト トラフィックをブロックするよう指定します。

デフォルト

不明なマルチキャストおよびユニキャスト トラフィックはブロックされていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、不明な MAC（メディア アクセス制御）アドレスを持ったすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャスト トラフィックはブロックすることができます。保護ポートで、不明なマルチキャストまたはユニキャスト トラフィックがブロックされない場合、セキュリティ上の問題が発生します。

不明なマルチキャストまたはユニキャスト トラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックに関する情報は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

例

次の例では、インターフェイス上で不明なマルチキャスト トラフィックをブロックする方法を示します。

```
Switch(config-if)# switchport block multicast
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。

switchport host

ホスト接続のためにポートを最適化するには、**switchport host** インターフェイス コンフィギュレーション コマンドを使用します。システム上への影響をなくすには、このコマンドの **no** 形式を使用します。

switchport host

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ポートのデフォルトは、ホストへの接続が最適化されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ホスト接続のためポートを最適化するには、**switchport host** コマンドでアクセスするスイッチ ポートモードを設定し、スパニング ツリー PortFast をイネーブルにし、チャネル グルーピングをディセーブルにします。エンド ステーションのみこの設定を適用することができます。

スパニング ツリー PortFast はイネーブルなので、**switchport host** コマンドを単一ホストと接続するポートにだけ入力します。その他のスイッチ、ハブ、コンセントレータ、またはブリッジと fast-start ポートを接続すると、一時的にスパニングツリー ループが発生することがあります。

switchport host コマンドをイネーブルにし、パケット転送の開始における遅延時間を減少させることができます。

例

次の例では、ポートのホスト接続の設定を最適化する方法を示します。

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	スイッチポート モードを含む、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。

switchport mode

ポートの VLAN メンバシップ モードを設定するには、**switchport mode** インターフェイス コンフィギュレーション コマンドを使用します。モードをデバイスの適切なデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

switchport mode {**access** | **dynamic** {**auto** | **desirable**} | **trunk**}

no switchport mode {**access** | **dynamic** | **trunk**}

シンタックスの説明

access	ポートをアクセス モード（**switchport access vlan** インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか）に設定します。ポートは無条件にアクセスするように設定され、非カプセル化（タグなし）フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN のみです。
dynamic auto	インターフェイス トランキング モード ダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチポート モードになります。
dynamic desirable	インターフェイス トランキング モード ダイナミック パラメータを desirable に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。
trunk	無条件にポートをトランクに設定します。ポートは VLAN レイヤ 2 インターフェイスをトランキングします。ポートは、送信元の VLAN を識別するカプセル化（タグ付き）フレームを送受信します。トランクは、2 つのスイッチ間、スイッチとルータ間のポイントツーポイント リンクです。

デフォルト

デフォルト モードは **dynamic auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

access または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して、適切なモードでポートを設定した場合のみです。スタティックアクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定のみです。

access モードを入力した場合、インターフェイスは固定的な非トランキング モードになり、近接インターフェイスがリンクから非トランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを入力した場合、インターフェイスは永続的なトランキング モードになり、接続先のインターフェイスが現在のリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを入力した場合に、ネイバー インターフェイスが **trunk** または **desirable** モードに設定されると、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを入力した場合に、ネイバー インターフェイスが **trunk**、**desirable**、または **auto** モードに設定されると、インターフェイスはトランク インターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN トランキング プロトコル（VTP）ドメインに存在する必要があります。トランク ネゴシエーションは、ポイントツーポイント プロトコルであるダイナミック トランキング プロトコル（DTP）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この事態を避けるには、DTP をサポートしない装置に接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンクを介してトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていない装置でトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

アクセス ポートとトランク ポートは、相互に排他的な関係にあります。

IEEE 802.1x 機能は、次の方法でスイッチポート モードに作用します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1x を **dynamic auto** または **dynamic desirable** にイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを **dynamic auto** または **dynamic desirable** ポートに変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス（VLAN Query Protocol [VQP]）ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

例

次の例では、ポートをアクセス モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode dynamic desirable
```

次の例では、ポートを trunk モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力し、Administrative Mode 行および Operational Mode 行の情報を調べます。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport access	ポートをスタティック アクセス ポートまたはダイナミック アクセス ポートとして設定します。
switchport trunk	インターフェイスがトランク モードの場合、トランクの特性を設定します。

switchport nonegotiate

レイヤ 2 インターフェイス上でダイナミック トランキング プロトコル（DTP）ネゴシエーション パケットが送信されないように指定するには、**switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用します。スイッチは、このインターフェイス上で DTP ネゴシエーションを行いません。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport nonegotiate

no switchport nonegotiate

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

nonegotiate ステータスを解除するには、**switchport nonegotiate** コマンドの **no** 形式を使用します。

このコマンドが有効なのは、インターフェイス スイッチポート モードがアクセスまたはトランク（**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定）の場合のみです。**dynamic**（**auto** または **desirable**）モードでこのコマンドを実行しようとすると、エラーが戻されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。デバイスは、**mode** パラメータ（**access** または **trunk**）に従って、トランキングを実行するかどうかを決定します。

- これらのリンクを介してトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスでのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

例

次の例では、ポートに対してトランキング モードのネゴシエートを制限し、（モードの設定に応じて）トランク ポートまたはアクセス ポートとして動作させる方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport nonegotiate
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport mode	ポートの VLAN メンバシップ モードを設定します。

switchport port-security

インターフェイス上でポート セキュリティをイネーブルにするには、キーワードなしで **switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。キーワードを指定すると、セキュア MAC（メディア アクセス制御）アドレス、スティッキ MAC アドレス ラーニング、セキュア MAC アドレスの最大数、または違反モードが設定されます。ポート セキュリティをディセーブルにするか、またはパラメータをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

no switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]

no switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown** | **shutdown vlan**}]

シンタックスの説明

aging	（任意）**switchport port-security aging** コマンドを参照してください。
mac-address *mac-address*	（任意）48 ビット MAC アドレスを入力して、インターフェイスのセキュア MAC アドレスを指定します。設定された最大値まで、セキュア MAC アドレスを追加できます。
vlan *vlan-id*	（任意）トランク ポート上でのみ、VLAN ID および MAC アドレスを指定します。VLAN ID が指定されない場合、ネイティブ VLAN が使用されます。
vlan access	（任意）アクセス ポートでのみ、VLAN をアクセス VLAN として指定します。
vlan voice	（任意）アクセス ポートでのみ、VLAN を音声 VLAN として指定します。 **（注）** **voice** キーワードは、音声 VLAN がポートに設定されてそのポートがアクセス VLAN でない場合のみ利用可能です。
mac-address sticky [*mac-address*]	（任意）インターフェイスの*スティッキ ラーニング*をイネーブルにするには、**mac-address sticky** キーワードのみを入力します。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習されたすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。 （任意）*mac-address* を入力し、スティッキ セキュア MAC アドレスを指定します。

maximum *value*	（任意）インターフェイスのセキュア MAC アドレスの最大数を設定します。スイッチで設定できるセキュア MAC アドレスの最大数は、システムで使用が許可されている MAC アドレスの最大数によって決まります。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他セキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。 デフォルトの設定は 1 です。
vlan [*vlan-list*]	（任意）トランク ポートに対して、VLAN のセキュア MAC アドレスの最大数を設定できます。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。 • **vlan** : VLAN ごとに最大値を設定します。 • **vlan** *vlan-list* : VLAN 範囲、または一連の VLAN 内の VLAN ごとに最大値を設定します。VLAN 範囲はハイフン、一連の VLAN はカンマで区切ります。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
violation	（任意）セキュリティ違反モード、またはポート セキュリティに違反した場合に実行するアクションを設定します。デフォルトは **shutdown** です。
protect	セキュリティ違反保護モードを設定します。このモードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュア MAC アドレス数を下げるか、許可するアドレスの最大数を増やさないかぎり、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。 **（注）** トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大制限に達していなくても VLAN が保護モードの最大制限に達すると、ラーニングがディセーブルになります。
restrict	セキュリティ違反制限モードを設定します。このモードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュア MAC アドレス数を下げるか、許可するアドレスの最大数を増やさないかぎり、この状態が続きます。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。
shutdown	セキュリティ違反シャットダウン モードを設定します。このモードでは、違反が発生し、ポートの LED がオフになると、インターフェイスが errdisable の状態になります。SNMP トラップが送信されます。また、Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除したり、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力したりして、手動で再びイネーブルにすることができます。
shutdown vlan	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。このモードでは、違反が発生した VLAN のみが errdisable になります。

デフォルト

ポート セキュリティはディセーブルです。

ポート セキュリティがイネーブルであり、キーワードが入力されていない場合、セキュア MAC アドレスの最大数のデフォルト値は 1 です。

デフォルトの違反モードは、**shutdown** です。

スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。
12.2(35)SE	**shutdown vlan** キーワードが追加されました。

使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートを Fast EtherChannel または Gigabit EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つを許可する十分なセキュア アドレスを設定する必要があります。
- 音声 VLAN はアクセス ポート上のみでサポートされます。トランク ポート上ではサポートされません。
- インターフェイスにセキュア アドレス最大値を入力した場合、新規の値が前回の値より大きいと、新規の値により、前回の設定値が無効にされます。新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキ セキュア MAC アドレスのポート セキュリティ エージングはサポートしていません。

セキュア MAC アドレスの最大値がアドレス テーブルに存在し、アドレス テーブルに存在しない MAC アドレスのステーションがインターフェイスにアクセスしようとする場合、または別のセキュア ポートのセキュア MAC アドレスとして設定された MAC アドレスを持ったステーションがインターフェイスにアクセスしようとする場合、セキュリティ違反が起こります。

セキュア ポートが errdisable ステートになっているときは、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

最大セキュア アドレスの値をインターフェイスに入力した場合、次の事象が発生します。

- 新しい値が古い値より大きい場合、新しい値が古い設定値を上書きします。
- 新しい値が古い値より小さく、インターフェイスで設定されていたセキュア アドレス数も新しい値より大きい場合、コマンドは拒否されます。

スティッキ セキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用し、インターフェイス上でスティッキ ラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミック セキュア MAC アドレスを（スティッキ ラーニングがイネーブルになる前にダイナミックに学習されたアドレスも含め）、スティッキ セキュア MAC アドレスに変換し、すべてのスティッキ セキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ ラーニングをディセーブルするか、または実行コンフィギュレーションを削除する場合、スティッキ セキュア MAC アドレスの一部は実行コンフィギュレーションのままですが、アドレス テーブルから削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、スティッキ セキュア MAC アドレスを設定する場合、アドレスはアドレス テーブルと実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスが保存されていない場合は、アドレスは失われます。スティッキ ラーニングをディセーブルにした場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。
- スティッキ ラーニングをディセーブルにして **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを入力した場合、エラー メッセージが表示され、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されません。

例

次の例では、ポート上でポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する方法を示します。違反モードがデフォルト モードであり、セキュア MAC アドレスが設定されていません。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

次の例では、ポート上でセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキ ラーニングをイネーブルにして、ポート上で 2 つのスティッキ セキュア MAC アドレスを入力する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

次の例では、違反が発生した場合に VLAN のみをシャットダウンするようにポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet 0/2
Switch(config)# switchport port-security violation shutdown vlan
```

設定を確認するには、**show port-security** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
clear port-security	MAC アドレス テーブルからスイッチ上またはインターフェイス上の特定のタイプのセキュア アドレスまたはすべてのセキュア アドレスを削除します。
show port-security address	スイッチで設定されるすべてのセキュア アドレスを表示します。
show port-security interface *interface-id*	スイッチまたは指定されたインターフェイスのポート セキュリティ設定を表示します。

switchport port-security aging

セキュア アドレス エントリのエージング タイムとタイプを設定したり、特定のポート上でのセキュア アドレスのエージング動作を変更したりするには、**switchport port-security aging** インターフェイス コンフィギュレーション コマンドを使用します。ポート セキュリティのエージングをディセーブルにしたり、パラメータをデフォルト状態に戻したりする場合は、このコマンドの **no** 形式を使用します。

switchport port-security aging {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

no switchport port-security aging {**static** | **time** | **type**}

シンタックスの説明

static	このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。
time *time*	このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。time が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された time（分）が経過したあとに期限切れとなり、セキュア アドレス リストから削除されます。
inactivity	非アクティブティ エージング タイプを設定します。指定された time 期間中にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。

デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルト期間は 0 分です。

デフォルトのエージング タイプは absolute です。

デフォルトのスタティック エージング動作はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

特定のポートのセキュア アドレス エージングをイネーブルにするには、ポート エージング タイムを 0 以外の値に設定します。

特定のセキュア アドレスに時間を限定してアクセスできるようにするには、エージング タイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュア アドレスが削除されます。

継続的にアクセスできるセキュア アドレス数を制限するには、エージング タイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュア アドレスが削除され、他のアドレスがセキュアになることができます。

セキュア アドレスのアクセス制限を解除するには、セキュア アドレスとして設定し、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュア アドレスのエージングをディセーブルにします。

例

次の例では、ポートのすべてのセキュア アドレスに対して、エージング タイプを absolute、エージング タイムを 2 時間に設定します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュア アドレスに対してエージングをイネーブルにし、inactivity タイプのエージングでエージング タイムを 2 分に設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュア アドレスに対してエージングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

関連コマンド

コマンド	説明
show port-security	ポートに定義されたポート セキュリティ設定を表示します。
switchport port-security	ポート上でポート セキュリティをイネーブルにし、ポートの使用対象をユーザ定義のステーション グループに制限し、セキュア MAC アドレスを設定します。

switchport priority extend

着信タグなしフレームのポート プライオリティを設定したり、指定のポートに接続された IP Phone が受信するフレームのプライオリティを設定したりするには、**switchport priority extend** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport priority extend {**cos** *value* | **trust**}

no switchport priority extend

（注）　このコマンドを使用するには、スイッチが LAN Base イメージを実行している必要があります。

シンタックスの説明

cos *value*	PC から受信したか、または特定のサービス クラス（CoS）値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ～ 7 です。7 が最も高いプライオリティになります。デフォルト値は 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

デフォルト

ポートで受信したタグのないフレームについて、デフォルト ポート プライオリティは、CoS 値 0 に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、スイッチを設定して、Cisco Discovery Protocol（CDP）パケットを送信し、Cisco IP Phone のアクセス ポートに接続する装置からデータ パケットを送信する方法を IP Phone に指示できます。Cisco IP Phone に設定を送信するには、Cisco IP Phone に接続するスイッチ ポートの CDP をイネーブルする必要があります （デフォルトにより、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです）。

スイッチ アクセス ポート上で音声 VLAN を設定する必要があります。

音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチの QoS（Quality of Service）をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するポート信頼状態を設定することを推奨します。

例

次の例では、受信された IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport priority extend trust
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces	スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport voice vlan {vlan-id | dot1p | none | untagged}	ポートに音声 VLAN を設定します。

switchport protected

同じスイッチ上で保護された他のポートから送信されるレイヤ 2 のユニキャスト、マルチキャスト、およびブロードキャスト トラフィックを分離するには、**switchport protected** インターフェイス コンフィギュレーション コマンドを使用します。ポートで保護をディセーブルにするには、このコマンドの **no** 形式を使用します。

switchport protected

no switchport protected

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

保護ポートは定義されていません。すべてのポートが保護されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

スイッチポート保護機能はスイッチに対してローカルです。同じスイッチ上の保護ポート間の通信は、レイヤ 3 デバイスを通してのみ行うことができます。異なるスイッチ上の保護ポート間の通信を禁止するには、各スイッチの保護ポートに一意の VLAN を設定し、スイッチ間にトランク リンクを設定する必要があります。保護ポートはセキュア ポートとは異なります。

保護ポートは、他の保護ポートにユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、PIM パケットなどの制御トラフィックのみが転送されます。保護ポート間を通過するすべてのデータ トラフィックはレイヤ 3 装置を介して転送されなければなりません。

モニタするポートおよびモニタされるポートの両方が保護ポートの場合、ポート モニタリングは機能しません。

例

次の例では、インターフェイス上で保護ポートをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport protected
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

シンタックスの説明

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport block	インターフェイス上で不明なユニキャストまたはマルチキャスト トラフィックを防ぎます。

switchport trunk

インターフェイスがトランキング モードの場合にトランクの特性を設定するには、**switchport trunk** インターフェイス コンフィギュレーション コマンドを使用します。トランキング特性をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

switchport trunk {**allowed vlan** *vlan-list* | **native vlan** *vlan-id* | **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan** | **native vlan** | {**pruning vlan**}

シンタックスの説明

allowed vlan *vlan-list*	トランキング モードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可 VLAN のリストを設定します。次の *vlan-list* 形式を参照してください。**none** キーワードは無効です。デフォルトは **all** です。
native vlan *vlan-id*	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です。
pruning vlan *vlan-list*	トランキング モードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。**all** キーワードは無効です。

vlan-list の形式は、**all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [**,***vlan-atom*...] です。各キーワードの意味は、次のとおりです。

- **all** は 1 ～ 4094 のすべての VLAN を示します。このキーワードは、リスト内のすべての VLAN を同時に設定することを許可していないコマンドでは使用できません。
- **none** は空のリストを意味します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** は現在設定されている VLAN リストを置き換えないで、定義済み VLAN リストを追加します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN ID（VLAN ID が 1005 より上）を使用できます。

  （注） 拡張範囲 VLAN は許可 VLAN リストには追加できますが、プルーニング適格 VLAN リストには追加できません。

  カンマを使い、連続しない VLAN ID を区切ります。指定の範囲の ID に対してはハイフンを使用します。

- **remove** は現在設定されている VLAN リストを置き換えないで、リストから定義済み VLAN リストを削除します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。

  （注） 許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。

  カンマを使い、連続しない VLAN ID を区切ります。指定の範囲の ID に対してはハイフンを使用します。

- **except** は定義済み VLAN リスト以外の、計算する必要がある VLAN を示します（指定した VLAN を除く VLAN が追加されます）。有効な ID は 1 ～ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。指定の範囲の ID に対してはハイフンを使用します。
- *vlan-atom* は、1 ～ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、より小さい値が最初になります（ハイフン区切り）。

デフォルト

VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。

すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

ネイティブ VLAN：

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブ モード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN：

- スパニングツリー ループまたはストームの危険性を減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol [CDP]、ポート集約プロトコル [PAgP]、Link Aggregation Control Protocol [LACP]、DTP、および VLAN 1 の VLAN トランキング プロトコル [VTP]）を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルト リスト（すべての VLAN を許可）にリセットします。

トランク プルーニング：

- プルーニング適格リストは、トランク ポートにだけ適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。
- VLAN 1、VLAN 1002 ～ 1005、および拡張範囲 VLAN（VLAN 1006 ～ 4094）は、プルーニングできません。

例

次の例では、VLAN 3 を、すべてのタグなしトラフィックを送信するデフォルト ポートに設定する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ～ 15 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces switchport	ポート ブロッキング、ポート保護設定など、スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport mode	ポートの VLAN メンバシップ モードを設定します。

switchport voice vlan

ポートに音声 VLAN を設定するには、**switchport voice vlan** interface インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged**}

no switchport voice vlan

シンタックスの説明

vlan-id	音声トラフィックに VLAN を使用するよう設定します。指定できる範囲は 1 ～ 4094 です。デフォルトでは、IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
untagged	IP Phone をタグなしの音声トラフィックを送信するよう設定します。これが IP Phone のデフォルト設定になります。

デフォルト

デフォルトでは、スイッチは IP Phone を自動設定しません（**none**）。

デフォルトでは、IP Phone はフレームにタグを付けません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

スイッチの Cisco IP Phone に接続しているスイッチ ポート上の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）をイネーブルにし、Cisco IP Phone に設定情報を送信する必要があります。インターフェイス上で CDP は、デフォルトの状態でグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**mls qos** グローバル コンフィギュレーション コマンドを入力してスイッチの QoS（Quality of Service）をイネーブルにし、**mls qos trust cos** インターフェイス コンフィギュレーション コマンドを入力して、信頼するポート信頼状態を設定することを推奨します。

VLAN ID を入力すると、IP Phone は指定された VLAN ID のタグが付けられた音声トラフィックを IEEE 802.1Q フレームで転送します。スイッチは IEEE 802.1Q 音声トラフィックを音声 VLAN に入れます。

dot1q、**none** または **untagged** を選択した場合、スイッチは指定の音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定する必要があります。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つを許可する十分なセキュア アドレスを設定する必要があります。

アクセス VLAN で任意のポート セキュリティ タイプがイネーブルにされた場合、音声 VLAN でダイナミック ポート セキュリティは自動的にイネーブルになります。

音声 VLAN では、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

例

次の例では、VLAN 2 をポート用音声 VLAN として設定します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport voice vlan 2
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces *interface-id* **switchport**	スイッチング ポートの管理ステータスおよび動作ステータスを表示します。
switchport priority extend	指定されたポートに接続されたデバイスが、着信ポートで受信したプライオリティ トラフィックを処理する方法を指定します。

system mtu

ギガビット イーサネット ポートまたはファスト イーサネット（10/100）ポートの最大パケット サイズや最大伝送ユニット（MTU）サイズを設定するには、**system mtu** グローバル コンフィギュレーション コマンドを使用します。グローバル MTU 値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system mtu {*bytes* | **jumbo** *bytes*}

no system mtu

シンタックスの説明

bytes	10 Mb/s または 100 Mb/s に設定されているポートのシステム MTU を設定します。指定できる範囲は 1500 ～ 1998 バイトです。これは、10/100 Mbps イーサネット スイッチ ポートで受信される最大 MTU です。
jumbo *bytes*	1000 Mbps 以上で稼動しているギガビット イーサネット ポートのシステム ジャンボ MTU を設定します。指定できる範囲は 1500 ～ 9000 バイトです。これは、ギガビット イーサネット ポートの物理ポートで受信される最大 MTU です。

デフォルト

すべてのポートのデフォルトの MTU サイズは 1500 バイトです。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンドでシステム MTU またはジャンボ MTU のサイズを変更した場合、新しい設定内容を反映させるには、スイッチをリセットする必要があります。システム MTU 設定は、NVRAM のスイッチ環境変数に保存され、スイッチがリロードした時点で有効になります。**system mtu** コマンドおよび **system mtu jumbo** コマンドで入力した MTU 設定は、**copy running-config startup-config** 特権 EXEC コマンドを入力しても、スイッチ IOS コンフィギュレーション ファイルに保存されません。したがって、TFTP を使用し、バックアップ コンフィギュレーション ファイルで新しいスイッチを設定して、システム MTU をデフォルト以外の値にしたい場合、新しいスイッチ上で **system mtu** および **system mtu jumbo** を明示的に設定し、スイッチをリロードする必要があります。

1000 Mbps で稼動しているギガビット イーサネット ポートは **system mtu** コマンドによる影響を受けません。10/100 Mbps ポートは **system mtu jumbo** コマンドによる影響を受けません。

指定されたスイッチ タイプの許容範囲外の値を入力すると、値が拒否されます。

（注）　スイッチは、インターフェイスごとの MTU の設定をサポートしません。

スイッチの CPU で受信できるフレーム サイズは、**system mtu** コマンドで入力した値に関係なく、1998 バイトに制限されています。転送されたフレームまたはルーテッド フレームは、通常 CPU では受信されませんが、一部のパケット（制御トラフィック、SNMP、Telnet、およびルーティング プロトコルなど）は CPU に送信されます。

たとえば、**system mtu** 値が 1998 バイトであり、**system mtu jumbo** 値が 5000 バイトである場合、1000 Mb/s で稼動しているインターフェイスでは、最大 5000 バイトのパケットを受信できます。ただし、1998 バイトを超えるパケットは 1000 Mb/s で稼動しているインターフェイスで受信できますが、宛先インターフェイスが 10 Mb/s または 100 Mb/s で稼動している場合はドロップされます。

例

次の例では、1000 Mbps 以上で稼動しているギガビット イーサネット ポートの最大ジャンボ パケット サイズを 1800 バイトに設定する方法を示します。

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

設定を確認するには、**show system mtu** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show system mtu	ファスト イーサネットおよびギガビット イーサネットのポートに設定されたパケット サイズを表示します。

test cable-diagnostics tdr

インターフェイス上で Time Domain Reflector（TDR）機能を実行するには、**test cable-diagnostics tdr** 特権 EXEC コマンドを使用します。

test cable-diagnostics tdr interface *interface-id*

シンタックスの説明

interface-id	TDR を実行するインターフェイスを指定します。

デフォルト

デフォルトはありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュール ポートではサポートされません。TDR の詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

test cable-diagnostics tdr interface *interface-id* コマンドを使用して TDR を実行したあと、結果を表示するには **show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを使用します。

例

次の例では、インターフェイス上で TDR を実行する方法を示します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

インターフェイスのリンク ステータスがアップであり、速度が 10 Mb/s または 100 Mb/s である場合、**test cable-diagnostics tdr interface** *interface-id* コマンドを入力すると次のメッセージが表示されます。

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

関連コマンド

コマンド	説明
show cable-diagnostics tdr	TDR 結果が表示されます。

traceroute mac

指定された送信元 MAC アドレスから指定された宛先 MAC アドレスまでのパケットがたどるレイヤ 2 パスを表示するには、**traceroute mac** 特権 EXEC コマンドを使用します。

traceroute mac [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

シンタックスの説明

interface *interface-id*	（任意）送信元および宛先スイッチ上のインターフェイスを指定します。
source-mac-address	送信元スイッチの MAC アドレスを指定します（16 進数）。
destination-mac-address	宛先スイッチの MAC アドレスを指定します（16 進数）。
vlan *vlan-id*	（任意）送信元スイッチから宛先スイッチを通過するパケットのレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID は 1 ～ 4094 です。
detail	（任意）詳細情報を表示するよう指定します。

デフォルト

デフォルトはありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、シスコ検出プロトコル（CDP）がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがパス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

レイヤ 2 traceroute はユニキャスト トラフィックのみをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、エラー メッセージが表示されます。

指定された送信元および宛先の MAC アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ 2 パスを表示します。異なる VLAN にある送信元および宛先 MAC アドレスを指定しても、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN にある場合、送信元および宛先 MAC アドレス両方の属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。

複数のデバイスがハブを通じて 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーが 1 つのポートで検知される場合）、レイヤ 2 traceroute の機能はサポートされません。1 つのポートで複数の CDP ネイバーが検知される場合、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用してレイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
C-12T / 2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元スイッチと宛先スイッチ上のインターフェイスを指定してレイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C2960-12T] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、該当するスイッチが送信元スイッチに接続されていない場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C2960-12T] (2.2.5.5)
con5 / WS-C2960-12T / 2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、該当するスイッチが送信元 MAC アドレス用の宛先ポートを検出できない場合のレイヤ 2 パスを示します。

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

次の例では、宛先 MAC アドレスがマルチキャスト アドレスの場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

次の例では、送信元および宛先スイッチが複数の VLAN にある場合のレイヤ 2 のパスを示しています。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
traceroute mac ip	指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

traceroute mac ip

指定された送信元 IP アドレスまたはホスト名から指定された宛先 IP アドレスまたはホスト名までのパケットがたどるレイヤ 2 パスを表示するには、**traceroute mac ip** 特権 EXEC コマンドを使用します。

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

シンタックスの説明

source-ip-address	送信元スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
destination-ip-address	宛先スイッチの IP アドレスを、32 ビットの値で指定します（ドット付き 10 進数）。
source-hostname	送信元スイッチの IP ホスト名を指定します。
destination-hostname	宛先スイッチの IP ホスト名を指定します。
detail	（任意）詳細情報を表示するよう指定します。

デフォルト

デフォルトはありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、シスコ検出プロトコル（CDP）がネットワークのすべてのスイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがパス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

パス内で識別できるホップ数は最大で 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定した場合、スイッチはアドレス解決プロトコル（ARP）を使用し、IP アドレスとそれに対応する MAC（メディア アクセス制御）アドレスおよび VLAN ID を関連付けます。

- 指定の IP アドレスの ARP のエントリが存在していた場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
- ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されないと、パスは識別されず、エラー メッセージが表示されます。

複数のデバイスがハブを通じて 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーが 1 つのポートで検知される場合）、レイヤ 2 traceroute の機能はサポートされません。1 つのポートで複数の CDP ネイバーが検知される場合、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、**detail** キーワードを使用して、送信元および宛先 IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C2960-12T / 2.2.6.6 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元と宛先のホスト名を指定してレイヤ 2 パスを表示する方法を示します。

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

関連コマンド

コマンド	説明
traceroute mac	指定された送信元 MAC アドレスから指定された宛先 MAC アドレスまでパケットがたどるレイヤ 2 パスを表示します。

trust

class ポリシー マップ コンフィギュレーション コマンドまたは **class-map** グローバル コンフィギュレーション コマンドで分類されたトラフィックの信頼状態を定義するには、**trust** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

trust [**cos** | **dscp** | **ip-precedence**]

no trust [**cos** | **dscp** | **ip-precedence**]

シンタックスの説明

cos	（任意）パケットのサービス クラス（CoS）値を使用して、入力パケットを分類します。タグのないパケットの場合、デフォルト ポートの CoS 値が使用されます。
dscp	（任意）パケットの Differentiated Service Code Point（DSCP）値（8 ビット サービス タイプ フィールドの上位 6 ビット）を使用することにより、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットにタグがない場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。
ip-precedence	（任意）パケットの IP precedence 値（8 ビット サービスタイプ フィールドの上位 3 ビット）を使用して、入力パケットを分類します。パケットにタグがある場合、非 IP パケットにはパケットの CoS 値が使用されます。パケットにタグがない場合、CoS の DSCP マッピングにデフォルト ポートの CoS 値が使用されます。

デフォルト

信頼できない状態です。キーワードが指定されず、コマンドが入力されている場合、デフォルトは **dscp** です。

コマンド モード

ポリシーマップ クラス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

特定のトラフィックの QoS（Quality of Service）の信頼動作を他のトラフィックと区別するために、このコマンドを使用します。たとえば、ある DSCP 値を持った着信トラフィックが信頼されます。着信トラフィックの DSCP 値と一致し、信頼できるクラス マップを設定できます。

このコマンドで設定された信頼性の値は、**mls qos trust** インターフェイス コンフィギュレーション コマンドで設定された信頼性の値を上書きします。

trust コマンドは、同一ポリシー マップ内の **set** ポリシーマップ クラス コンフィギュレーション コマンドと相互に排他的な関係にあります。

trust cos を指定した場合、QoS は受信した、またはデフォルト ポートの CoS 値および CoS/DSCP マップを使用し、パケットの DSCP 値を生成します。

trust dscp を指定した場合、QoS は入力パケットから DSCP 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値、タグなしの非 IP パケットに対しては、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

trust ip-precedence を指定した場合、QoS は入力パケットおよび IP precedence/DSCP マップから IP precedence 値を使用します。タグ付きの非 IP パケットに対しては、QoS は受信した CoS 値、タグなしの非 IP パケットに対しては、デフォルト ポートの CoS 値を使用します。どちらの場合も、パケットの DSCP 値は CoS/DSCP マップから抽出されます。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、*class1* で分類されたトラフィックの着信 DSCP 値を信頼するため、ポート信頼状態を定義する方法を示します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
class	指定されたクラスマップ名のトラフィック分類一致条件（**police**、**set**、および **trust** ポリシーマップ クラス コンフィギュレーション コマンドによる）を定義します。
police	分類したトラフィックにポリサーを定義します。
policy-map	複数のポートに適用することによってサービス ポリシーを指定できるポリシー マップを作成または変更します。
set	パケットに DSCP 値または IP precedence 値を設定することによって、IP トラフィックを分類します。
show policy-map	QoS ポリシー マップを表示します。

udld

単方向リンク検出（UDLD）でアグレッシブ モードまたはノーマル モードをイネーブルにし、設定可能なメッセージ タイマー時間を設定するには、**udld** グローバル コンフィギュレーション コマンドを使用します。すべての光ファイバ ポートでアグレッシブ モードまたはノーマル モードの UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。

udld {**aggressive** | **enable** | **message time** *message-timer-interval*}

no udld {**aggressive** | **enable** | **message**}

シンタックスの説明

aggressive	すべての光ファイバ インターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。
enable	すべての光ファイバ インターフェイスにおいて、ノーマル モードで UDLD をイネーブルにします。
message time *message-timer-interval*	アドバタイズ フェーズにあり、双方向と判別されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 7 ～ 90 秒です。

デフォルト

すべてのインターフェイスで UDLD はディセーブルです。

メッセージ タイマーは 60 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

UDLD は、ノーマル モード（デフォルト）とアグレッシブ モードという 2 つの動作モードをサポートしています。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。ノーマル モードとアグレッシブ モードの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Understanding UDLD」を参照してください。

プローブ パケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷のトレードオフを行っていることになります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバ インターフェイスだけです。他のインターフェイス タイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD によるインターフェイス シャットダウンをリセットするのに、以下のコマンドを使用できます。

- **udld reset** 特権 EXEC コマンド - UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドのあとに **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを入力 - グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドのあとに **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力 - 指定されたインターフェイスの UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド - 自動的に UDLD errdisable ステートから回復します。

例

次の例では、すべての光ファイバ インターフェイスで UDLD をイネーブルにする方法を示します。

```
Switch(config)# udld enable
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show udld	すべてのポートまたは指定されたポートの UDLD 管理上および運用上のステータスを表示します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。
udld reset	UDLD によってシャットダウンされたすべてのインターフェイスをリセットし、トラフィックが再び通過するのを許可します。

udld port

個々のインターフェイス上で UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドでイネーブルにならないようにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。**udld** グローバル コンフィギュレーション コマンド設定に戻したり、非光ファイバ ポートで入力された場合に UDLD をディセーブルしたりする場合は、このコマンドの **no** 形式を使用します。

udld port [**aggressive**]

no udld port [**aggressive**]

シンタックスの説明

aggressive	指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

デフォルト

光ファイバ インターフェイスでは、UDLD はイネーブル、アグレッシブ モード、ディセーブルのいずれでもありません。このため、光ファイバ インターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに従い UDLD をイネーブルにします。

非光ファイバ インターフェイスでは、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合は、このポートは単一方向リンクを検出できません。

UDLD は、ノーマル モード（デフォルト）とアグレッシブ モードという 2 つの動作モードをサポートしています。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。ノーマル モードとアグレッシブ モードの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring UDLD」の章を参照してください。

UDLD をノーマル モードでイネーブルにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。UDLD をアグレッシブ モードでイネーブルにするには、**udld port aggressive** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no udld port** コマンドを使用します。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を無効にする場合は、光ファイバ ポートで **udld port aggressive** コマンドを使用します。設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no** 形式を使用します。

UDLD によるインターフェイス シャットダウンをリセットするのに、以下のコマンドを使用できます。

- **udld reset** 特権 EXEC コマンド - UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンド
- **no udld enable** グローバル コンフィギュレーション コマンドのあとに **udld** {**aggressive** | **enable**} グローバル コンフィギュレーション コマンドを入力 - グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドのあとに **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力 - 指定されたインターフェイスの UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド - 自動的に UDLD errdisable ステートから回復します。

例

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション コマンドの設定に関係なく、光ファイバ インターフェイス上で UDLD をディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld** *interface* 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
show udld	すべてのポートまたは指定されたポートの UDLD 管理上および運用上のステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld reset	UDLD によってシャットダウンされたすべてのインターフェイスをリセットし、トラフィックが再び通過するのを許可します。

udld reset

単一方向リンク検出（UDLD）によってディセーブルになったインターフェイスをすべてリセットし、トラフィックの転送を再び許可するには、**udld reset** 特権 EXEC コマンドを使用します（イネーブルの場合には、スパニング ツリー、ポート集約プロトコル [PAgP]、Dynamic Trunking Protocol [DTP] などの他の機能が有効になります）。

udld reset

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

インターフェイスの設定で、UDLD がまだイネーブルである場合、これらのポートは再び UDLD の稼動を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

例

次の例では、UDLD によってディセーブルにされたすべてのインターフェイスをリセットする方法を示します。

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show running-config	スイッチの実行コンフィギュレーションを表示します。構文情報については、「Cisco IOS Configuration Fundamentals Command Reference, Release 12.2」>「File Management Commands」>「Configuration File Management Commands」を選択してください。
show udld	すべてのポートまたは指定されたポートの UDLD 管理上および運用上のステータスを表示します。
udld	UDLD のアグレッシブ モードまたはノーマル モードをイネーブルにするか、または設定可能なメッセージ タイマーの時間を設定します。
udld port	個々のインターフェイスで UDLD をイネーブルにするか、または光ファイバ インターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぎます。

vlan（グローバル コンフィギュレーション）

VLAN を追加して config-vlan モードを開始するには、**vlan** グローバル コンフィギュレーション コマンドを使用します。VLAN を削除する場合は、このコマンドの **no** 形式を使用します。標準範囲 VLAN（VLAN ID 1 ～ 1005）のコンフィギュレーション情報は、常に VLAN データベースに保存されます。VLAN トランキング プロトコル（VTP ）モードが透過の場合は、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成できます。これにより、VTP モード、ドメイン名、および VLAN 設定がスイッチ実行コンフィギュレーション ファイルに保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用すれば、設定をスイッチ スタートアップ コンフィギュレーション ファイルに保存できます。

vlan *vlan-id*

no vlan vlan-*id*

シンタックスの説明

vlan-id	追加および設定する VLAN の ID。*vlan-id* に指定できる範囲は 1 ～ 4094 です。VLAN ID を単独で入力したり、それぞれをカンマで区切って一連の VLAN ID を入力したり、ハイフンを間に挿入して VLAN ID の範囲を入力したりすることができます。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を追加するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用する必要があります。拡張範囲で VLAN を設定する前に、**vtp transparent** グローバル コンフィギュレーション コマンドまたは VLAN コンフィギュレーション コマンドを使用してスイッチを VTP 透過モードにします。拡張範囲 VLAN は、VTP によって学習されず、VLAN データベースにも追加されませんが、VTP モードが透過型である場合には、VTP モード、ドメイン名、およびすべての VLAN 設定は、実行コンフィギュレーションに保存され、これをスイッチ スタートアップ コンフィギュレーション ファイルに保存することもできます。

VLAN 設定と VTP 設定をスタートアップ コンフィギュレーション ファイルに保存してスイッチを再起動すると、設定が次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- VTP モードがサーバの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 個の VLAN の VTP モードおよび VLAN 設定には VLAN データベース情報が使用されます。

スイッチが VTP 透過モードでない場合に拡張範囲 VLAN を作成しようとすると、VLAN は拒否され、エラー メッセージが表示されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、config-vlan モードを開始できません。

vlan コマンドを VLAN ID とともに入力すると、config-vlan モードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、config-vlan モードを終了したときに追加または変更されます。（VLAN 1 ～ 1005 の）**shutdown** コマンドだけがただちに有効になります。

次のコンフィギュレーション コマンドが config-vlan モードで利用できます。このコマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。

（注） すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされている VLAN コンフィギュレーション コマンドは **mtu** *mtu-size* と **remote-span** だけです。拡張範囲 VLAN の場合、他のすべての特性はデフォルト ステートのままにしておく必要があります。

- **are** *are-number*：この VLAN の All-Route Explorer（ARE）ホップの最大数を定義します。このキーワードは、TrCRF VLAN にだけ適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。値が入力されていない場合は、0 が最大数と見なされます。
- **backupcrf**：バックアップ CRF モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
  - この VLAN のバックアップ CRF モードを **enable**（イネーブル）にします。
  - この VLAN のバックアップ CRF モードを **disable**（ディセーブル）にします（デフォルト）。
- **bridge** {*bridge-number*| **type**}：論理分散ソース ルーティング ブリッジ（つまり、FDDI-NET、トークンリング NET、および TrBRF VLAN 内でこの VLAN が親 VLAN として設定されているすべての論理リングと相互接続するブリッジ）を指定します。指定できる範囲は 0 ～ 15 です。FDDI-NET、TrBRF、およびトークンリング NET VLAN のデフォルト ブリッジ番号は 0（ソースルーティング ブリッジなし）です。**type** キーワードは、TrCRF VLAN にだけ適用され、次のうちの 1 つです。
  - **srb**（Source-Route Bridge [SRB; ソースルート ブリッジ]）
  - **srt**（ソースルート トランスペアレント [SRT]）ブリッジング VLAN
- **exit**：変更を適用し、VLAN データベース リビジョン番号（VLAN 1 ～ 1005 のみ）を増分して、config-vlan モードを終了します。
- **media**：VLAN メディア タイプを定義します。さまざまなメディア タイプで有効なコマンドおよび構文については、表 2-41 を参照してください。

  （注） スイッチがサポートするのは、イーサネット ポートだけです。FDDI およびトークンリング メディア固有の特性は、別のスイッチに対する VLAN トランキング プロトコル（VTP）グローバル アドバタイズにかぎって設定します。これらの VLAN はローカルに停止されます。

  - **ethernet** は、イーサネット メディア タイプです（デフォルト）。
  - **fddi** は、FDDI メディア タイプです。
  - **fd-net** は、FDDI-NET メディア タイプです。
  - **tokenring** は、VTP v2 モードがディセーブルの場合にはトークンリング メディア タイプであり、VTP v 2 モードがイネーブルの場合は TrCRF です。

  - **tr-net** は、VTP v2 モードがディセーブルの場合にはトークンリング NET メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。

- **mtu** *mtu-size* : MTU を指定します（バイト単位のパケット サイズ）。指定できる範囲は 1500 ～ 18190 です。デフォルト値は 1500 バイトです。
- **name** *vlan-name* : 管理ドメイン内で一意にする必要のある VLAN 名を 1 ～ 32 文字の ASCII 文字列で指定します。デフォルトは *VLANxxxx* です。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。
- **no** : コマンドを無効にするか、デフォルト設定に戻します。
- **parent** *parent-vlan-id* : 既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定します。このパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときに必要です。指定できる範囲は 0 ～ 1005 です。FDDI およびトークンリング VLAN のデフォルトの親 VLAN ID は 0（親 VLAN なし）です。トークンリングおよび TrCRF VLAN では、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。
- **remote-span** : VLAN をリモート SPAN（RSPAN）VLAN として設定します。RSPAN 機能が既存の VLAN に追加される場合、まず VLAN は削除され、次に RSPAN 機能とともに再生されます。RSPAN 機能が削除されるまで、どのアクセス ポートも非アクティブ化されます。VTP がイネーブルの場合、新しい RSPAN VLAN は、VLAN ID が 1024 より小さい VLAN 用の VTP で伝播されます。ラーニングは VLAN 上でディセーブルになります。詳細については、**remote-span** コマンドを参照してください。
- **ring** *ring-number* : FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ～ 4095 です。トークンリング VLAN のデフォルト値は 0 です。FDDI VLAN には、デフォルト値がありません。
- **said** *said-value* : IEEE 802.10 に記載されている Security Association Identifier（SAID）を指定します。指定できる ID は、1 ～ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000 に VLAN ID 番号を加算した値です。
- **shutdown** : VLAN 上で VLAN スイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、config-vlan モードを終了したときに有効になります。
- **state** : VLAN ステートを指定します。
  - **active** は、VLAN が稼動中であることを意味します（デフォルト）。
  - **suspend** は、VLAN が停止していることを意味します。停止している VLAN はパケットを通過させません。
- **ste** *ste-number* : Spanning-Tree Explorer（STE; スパニングツリー エクスプローラ）ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。
- **stp type** : FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリー タイプを定義します。FDDI-NET VLAN の場合、STP タイプは **ieee** です。トークンリング NET VLAN の場合、デフォルトの STP タイプは **ibm** です。FDDI およびトークンリング VLAN の場合、デフォルトのタイプは指定されていません。
  - SRT ブリッジングを実行している IEEE イーサネット STP の場合は、**ieee**
  - SRB を実行している IBM STP の場合は、**ibm**
  - SRT ブリッジング（IEEE）および SRB（IBM）の組み合わせを実行している STP の場合は、**auto**

- **tb-vlan1** *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id*：この VLAN とのトランスレーショナル ブリッジングが最初に実行される VLAN と 2 番めに実行される VLAN を指定します。トランスレーショナル VLAN は、たとえば FDDI またはトークンリングをイーサネットに変換します。指定できる範囲は 0 ～ 1005 です。値が指定されていない場合は、0（トランスレーショナル ブリッジングなし）と見なされます。

表 2-41　さまざまなメディア タイプに有効なコマンドと構文

メディア タイプ	指定できる構文
イーサネット	**name** *vlan-name*、**media ethernet**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**remote-span**、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
FDDI	**name** *vlan-name*、**media fddi**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**ring** *ring-number*、**parent** *parent-vlan-id*、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
FDDI-NET	**name** *vlan-name*、**media fd-net**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**bridge** *bridge-number*、**stp type** {**ieee** | **ibm** | **auto**}、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id* VTP v2 モードがディセーブルの場合、**stp type** を **auto** に設定しないでください。
トークンリング	VTP v1 モードはイネーブルです。 **name** *vlan-name*、**media tokenring**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**ring** *ring-number*、**parent** *parent-vlan-id*、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
TrCRF	VTP v2 モードはイネーブルです。 **name** *vlan-name*、**media tokenring**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**ring** *ring-number*、**parent** *parent-vlan-id*、**bridge type** {**srb** | **srt**}、**are** *are-number*、**ste** *ste-number*、**backupcrf** {**enable** | **disable**}、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
トークンリング NET	VTP v1 モードはイネーブルです。 **name** *vlan-name*、**media tr-net**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**bridge** *bridge-number*、**stp type** {**ieee** | **ibm**}, **tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*
TrBRF	VTP v2 モードはイネーブルです。 **name** *vlan-name*、**media tr-net**、**state** {**suspend** | **active**}、**said** *said-value*、**mtu** *mtu-size*、**bridge** *bridge-number*、**stp type** {**ieee** | **ibm** | **auto**}、**tb-vlan1** *tb-vlan1-id*、**tb-vlan2** *tb-vlan2-id*

表 2-42 に、VLAN の設定規則を示します。

表 2-42　VLAN 設定規則

設定	規則
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。 リング番号を指定します。このフィールドを空白のままにしないでください。 各 TrCRF VLAN の親 VLAN ID が同じ場合に一意のリング番号を指定します。1 つのバックアップ Concentrator Relay Function（CRF; コンセントレータ リレー機能）だけをイネーブルにすることができます。
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしないでください。
VTP v1 モードがイネーブルの場合	VLAN の STP タイプを auto に設定しないでください。 この規則は、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。
トランスレーショナル ブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）	使用されるトランスレーショナル ブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 （たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナル ブリッジング VLAN ID にも、トランスレーショナル ブリッジング パラメータの 1 つに元の VLAN へのポインタが含まれている必要があります。 コンフィギュレーションがポイントするトランスレーショナル ブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）元の VLAN とは異なったメディア タイプである必要があります。 両方のトランスレーショナル ブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なったメディア タイプである必要があります。

例

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには *VLANxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。デフォルトの **media** オプションは **ethernet** です。**state** オプションは **active** です。デフォルトの *said-value* 変数は、100000 に VLAN ID を加算した値です。*mtu-size* 変数は 1500、**stp-type** オプションは **ieee** です。**exit** config-vlan コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何もしません。

次の例では、新しい VLAN をすべてデフォルト特性で作成し、config-vlan モードを開始する方法を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

次の例では、すべての特性がデフォルトである拡張範囲 VLAN を新規作成し、config-vlan モードを開始して、新規 VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する方法を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan	すべての設定された VLAN または 1 つの VLAN（VLAN ID または名前が指定されている場合）のパラメータを管理ドメインに表示します。
vlan（VLAN コンフィギュレーション）	標準範囲 VLAN を VLAN データベースに設定します。

vlan（VLAN コンフィギュレーション）

VLAN データベースに標準範囲 VLAN（VLAN ID 1 ～ 1005）の VLAN 特性を設定するには、**vlan** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** 特権 EXEC コマンドを入力します。VLAN を削除する場合は、追加パラメータなしでこのコマンドの **no** 形式を使用します。設定された特性を変更する場合は、パラメータとともにこのコマンドの **no** 形式を使用します。

vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** mtu-size] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id]*

no vlan *vlan-id* [**are** *are-number*] [**backupcrf** {**enable** | **disable**}] [**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *said-value*] [**state** {**suspend** | **active**}] [**ste** *ste-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

拡張範囲 VLAN（VLAN ID 1006 ～ 4094）は、これらのコマンドを使用して追加することも変更することもできません。拡張範囲 VLAN を追加する場合は、**vlan（グローバル コンフィギュレーション）** コマンドを使用して config-vlan モードを開始します。

（注）　スイッチがサポートするのは、イーサネット ポートだけです。FDDI およびトークンリング メディア固有の特性は、別のスイッチに対する VLAN トランキング プロトコル（VTP）グローバル アドバタイズにかぎって設定します。これらの VLAN はローカルに停止されます。

シンタックスの説明

vlan-id	設定された VLAN の ID。指定できる ID は、1 ～ 1005 です。この数字は、管理ドメイン内で一意である必要があります。先行ゼロは入力しないでください。
are *are-number*	（任意）この VLAN の All-Route Explorer（ARE）ホップの最大数を指定します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。値が入力されていない場合は、0 が最大数と見なされます。
backupcrf {**enable** | **disable**}	（任意）バックアップ コンセントレータ リレー機能（CRF）モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。 • この VLAN のバックアップ CRF モードを **enable**（イネーブル）にします。 • この VLAN のバックアップ CRF モードを **disable**（ディセーブル）にします。

bridge *bridge-number* | **type** {**srb** | **srt**}	（任意）論理分散ソース ルーティング ブリッジ、つまり FDDI-Network Entity Title（NET）、トークンリング NET、および Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。 指定できる範囲は 0 ～ 15 です。 **type** キーワードは、TrCRF VLAN にだけ適用され、次のうちの 1 つです。 • **srb**（ソースルート ブリッジ [SRB]） • **srt**（ソースルート トランスペアレント [SRT]）ブリッジング VLAN
media {**ethernet** | **fddi** | **fd-net** | **tokenring** | **tr-net**}	（任意）VLAN メディア タイプを指定します。表 2-43 に、各メディア タイプに有効な構文を示します。 • **ethernet** は、イーサネット メディア タイプです（デフォルト）。 • **fddi** は、FDDI メディア タイプです。 • **fd-net** は、FDDI-NET メディア タイプです。 • **tokenring** は、VTP v2 モードがディセーブルの場合にはトークンリング メディア タイプであり、VTP v2 モードがイネーブルの場合は TrCRF です。 • **tr-net** は、VTP v2 モードがディセーブルの場合にはトークンリング NET メディア タイプであり、VTP v2 モードがイネーブルの場合は TrBRF メディア タイプです。
mtu *mtu-size*	（任意）最大伝送ユニット（MTU）（バイト単位のパケットサイズ）を指定します。指定できる範囲は 1500 ～ 18190 です。
name *vlan-name*	（任意）管理ドメイン内で一意である 1 ～ 32 文字の ASCII 文字列で VLAN 名を指定します。
parent *parent-vlan-id*	（任意）既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定します。このパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときに必要です。指定できる範囲は 0 ～ 1005 です。
ring *ring-number*	（任意）FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ～ 4095 です。
said *said-value*	（任意）IEEE 802.10 に記載されている Security Association Identifier（SAID）を指定します。指定できる ID は、1 ～ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。
state {**suspend** | **active**}	（任意）VLAN ステートを指定します。 • **active** である場合、VLAN は稼動中です。 • **suspend** の場合、VLAN は停止しています。停止している VLAN はパケットを通過させません。
ste *ste-number*	（任意）STE（スパニングツリー エクスプローラ）ホップの最大数を指定します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。

stp type {**ieee** | **ibm** | **auto**}	（任意）FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリー タイプを指定します。 • SRT ブリッジングを実行している IEEE イーサネット STP の場合は、**ieee** • SRB を実行している IBM STP の場合は、**ibm** • SRT ブリッジング（IEEE）および SRB（IBM）の組み合わせを実行している STP の場合は、**auto**
tb-vlan1 *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id*	（任意）この VLAN にトランスレーショナル ブリッジングが行われている 1 番めおよび 2 番めの VLAN を指定します。トランスレーショナル VLAN は、たとえば FDDI またはトークンリングをイーサネットに変換します。指定できる範囲は 0 ～ 1005 です。値が指定されていない場合は、0 と見なされます。

表 2-43 に、さまざまなメディア タイプで指定できる構文オプションを示します。

表 2-43　さまざまなメディア タイプに有効な構文

メディア タイプ	指定できる構文
イーサネット	**vlan** *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI	**vlan** *vlan-id* [**name** *vlan-name*] **media fddi** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI-NET	**vlan** *vlan-id* [**name** *vlan-name*] **media fd-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*] VTP v2 モードがディセーブルの場合、**stp type** を **auto** に設定しないでください。
トークンリング	VTP v1 モードはイネーブルです。 **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
TrCRF	VTP v2 モードはイネーブルです。 **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**bridge type** {**srb** | **srt**}] [**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
トークンリング NET	VTP v1 モードはイネーブルです。 **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
TrBRF	VTP v2 モードはイネーブルです。 **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

表 2-44 に、VLAN の設定規則を示します。

表 2-44　VLAN 設定規則

設定	規則
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。 リング番号を指定します。このフィールドを空白のままにしないでください。 各 TrCRF VLAN の親 VLAN ID が同じ場合に一意のリング番号を指定します。1 つのバックアップ コンセントレータ リレー機能（CRF）だけをイネーブルにすることができます。
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしないでください。
VTP v1 モードがイネーブルの場合	VLAN の STP タイプを auto に設定しないでください。 この規則は、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。
トランスレーショナル ブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）	使用されるトランスレーショナル ブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 （たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナル ブリッジング VLAN ID にも、トランスレーショナル ブリッジング パラメータの 1 つに元の VLAN へのポインタが含まれている必要があります。 コンフィギュレーションがポイントするトランスレーショナル ブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）元の VLAN とは異なったメディア タイプである必要があります。 両方のトランスレーショナル ブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なったメディア タイプである必要があります。

デフォルト

ARE 値は 7 です。

バックアップ CRF はディセーブルです。

FDDI-NET、TrBRF、およびトークンリング NET VLAN については、ブリッジ番号は 0（ソース ルーティング ブリッジなし）です。

media タイプは **ethernet** です。

デフォルトの *mtu size* は 1500 バイトです。

vlan-name 変数は *VLANxxxx* です。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。

親 VLAN ID は、FDDI およびトークンリング VLAN では 0（親 VLAN なし）です。TrCRF VLAN では、親 VLAN ID を指定する必要があります。トークンリングおよび TrCRF VLAN では、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。

トークンリング VLAN の *ring number* は 0 です。FDDI VLAN には、デフォルト値がありません。

said value は、100000 に VLAN ID 番号を加算した値です。

ステートは **active** です。

STE 値は 7 です。

STP タイプは、FDDI-NET では **ieee**、トークンリング NET VLAN では **ibm** です。FDDI およびトークンリング VLAN の場合、デフォルトのタイプは指定されていません。

tb-vlan1-id および *tb-vlan2-id* 変数は 0（トランスレーショナル ブリッジングなし）です。

コマンド モード

VLAN コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

このコマンド モードを使用できるのは、標準範囲 VLAN（VLAN ID 1 ～ 1005）を設定する場合だけです。

（注）拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を設定する場合は、**vlan** グローバル コンフィギュレーション コマンドを使用してください。

VTP の設定は常に VLAN データベースに保存されます。VTP モードが透過型の場合、VTP 設定は、VTP モードおよびドメイン名とともにスイッチの実行コンフィギュレーション ファイルにも保存されます。**copy running-config startup-config** 特権 EXEC コマンドを使用すれば、これをスイッチ スタートアップ コンフィギュレーション ファイルに保存できます。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存してスイッチを再起動した場合、設定は次のように選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- VTP モードがサーバである場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VLAN の VTP モードおよび VTP 設定には VLAN データベース情報が使用されます。

no vlan コマンドを使用した結果は次のとおりです。

- **no vlan** *vlan-id* 形式を使用すると、VLAN は削除されます。VLAN を削除すると、削除された VLAN を参照する他の親 VLAN およびトランスレーショナル ブリッジング パラメータは自動的に 0 にリセットされます。
- **no vlan** *vlan-id* **bridge** 形式を使用すると、VLAN ソース ルーティング ブリッジ番号はデフォルトの 0 に戻ります。**vlan** *vlan-id* **bridge** コマンドは、FDDI-NET およびトークンリング NET VLAN でのみ使用され、他の VLAN タイプでは無視されます。
- **no vlan** *vlan-id* **media** 形式を使用すると、メディア タイプはデフォルト（**ethernet**）に戻ります。VLAN メディア タイプ（**no** 形式を含む）を変更すると、（そのコマンドに **mtu** キーワードも存在しない場合）VLAN MTU はそのタイプのデフォルトの MTU にリセットされます。また、VLAN の親 VLAN およびトランスレーショナル ブリッジング VLAN も（そのコマンドに **parent**、**tb-vlan1** または **tb-vlan2** も存在しない場合）デフォルトにリセットされます。
- **no vlan** *vlan-id* **mtu** 形式を使用すると、VLAN MTU は適用可能な VLAN メディア タイプのデフォルトに戻ります。**media** キーワードを使用しても MTU を変更できます。
- **no vlan** *vlan-id* **name** *vlan-name* 形式を使用すると、VLAN 名はデフォルト名に戻ります（*VLANxxxx*、ここで *xxxx* は VLAN ID 番号に等しい 4 桁の数字 [先行ゼロを含む] です）。
- **no vlan** *vlan-id* **parent** 形式を使用すると、親 VLAN はデフォルト（0）に戻ります。親 VLAN が削除された場合、または **media** キーワードによって VLAN タイプまたは親 VLAN の VLAN タイプが変更された場合、親 VLAN はデフォルトにリセットされます。
- **no vlan** *vlan-id* **ring** 形式を使用すると、VLAN 論理リング番号はデフォルト（0）に戻ります。
- **no vlan** *vlan-id* **said** 形式を使用すると、VLAN SAID はデフォルト（100000 に VLAN ID を加算した値）に戻ります。
- **no vlan** *vlan-id* **state** 形式を使用すると、VLAN ステートはデフォルト（**active**）に戻ります。
- **no vlan** *vlan-id* **stp type** 形式を使用すると、VLAN スパニングツリー タイプはデフォルト（**ieee**）に戻ります。
- **no vlan** *vlan-id* **tb-vlan1** または **no** *-id* **tb-vlan2** 形式を使用すると、1 つまたは複数の VLAN トランスレーショナル ブリッジ VLAN はデフォルト（0）に戻ります。トランスレーショナル ブリッジ VLAN は、影響を受ける VLAN とは異なった VLAN タイプである必要があります。2 つ指定した場合には、この 2 つが互いに異なった VLAN タイプである必要があります。トランスレーショナル ブリッジ VLAN が削除された場合、**media** キーワードにより VLAN タイプが変更された場合、または **media** キーワードにより対応するトランスレーション ブリッジ VLAN の VLAN タイプが変更された場合、トランスレーショナル ブリッジ VLAN はデフォルトに戻ります。

例

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには *VLANxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。デフォルトの **media** オプションは **ethernet** です。**state** オプションは **active** です。デフォルトの *said-value* 変数は、100000 に VLAN ID を加算した値です。*mtu-size* 変数は 1500、**stp-type** オプションは **ieee** です。**exit** または **apply** vlan コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何も作用しません。

```
Switch(vlan)# vlan 2
VLAN 2 added:
    Name: VLAN0002
Switch(vlan)# exit
APPLY completed.
Exiting....
```

次の例では、名前および MTU サイズを変更することにより既存の VLAN を変更する方法を示します。

```
Switch(vlan)# no vlan name engineering mtu 1200
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vlan	すべての設定された VLAN または 1 つの VLAN（VLAN ID または名前が指定されている場合）のパラメータを管理ドメインに表示します。
vlan（グローバル コンフィギュレーション）	標準範囲および拡張範囲 VLAN を設定するための config-vlan モードを開始します。

vlan database

VLAN コンフィギュレーション モードを開始するには、**vlan database** 特権 EXEC コマンドを入力します。このモードから、標準範囲 VLAN の VLAN 設定の追加、削除、および変更を行い、VLAN トランキング プロトコル（VTP）を使用してこれらの変更をグローバルに伝播できます。コンフィギュレーション情報は、VLAN データベースに保存されます。

vlan database

（注）　VLAN コンフィギュレーション モードは、VLAN ID が 1 ～ 1005 の VLAN にのみ有効となります。

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VLAN データベース コンフィギュレーション コマンドを使用すると、VLAN 1 ～ 1005 を設定できます。拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を設定するには、**vlan（グローバル コンフィギュレーション）** コマンドを使用して config-vlan モードを開始します。また、**vlan** グローバル コンフィギュレーション コマンドを使用して VLAN ID 1 ～ 1005 を設定することもできます。

VLAN コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

（注）　このコマンド モードはセッション指向であるため、他のモードとは異なっています。VLAN パラメータを追加、削除、または変更した場合、**apply** または **exit** コマンドを入力してセッションを終了するまでその変更は適用されません。変更が適用されると、VTP コンフィギュレーション バージョンは増分されます。*abort* を入力して変更を VTP データベースに適用しないこともできます。

VLAN コンフィギュレーション モードに入っている場合は、VLAN データベースにアクセスし、次のコマンドを使用して変更を加えることができます。

- **vlan**：サブコマンドにアクセスして、1 つの VLAN に関連付けられた値を追加、削除、または変更します。詳細については、**vlan（VLAN コンフィギュレーション）** コマンドを参照してください。
- **vtp**：サブコマンドにアクセスして、VTP 管理機能を実行します。詳細については、**vtp（VLAN コンフィギュレーション）** コマンドを参照してください。

VLAN または VTP パラメータを変更した場合、次の編集バッファ処理コマンドを使用できます。

- **abort**：変更を適用せずにこのモードを終了します。VLAN コンフィギュレーション モードを開始する前に稼動していた VLAN 設定を引き続き使用します。
- **apply**：現在の変更を VLAN データベースに適用し、データベース コンフィギュレーション リビジョン番号を増分し、管理ドメイン全体にこれを伝播し、VLAN コンフィギュレーション モードを継続します。

（注）　スイッチが VTP クライアント モードである場合にはこのコマンドを使用することはできません。

- **exit**：すべてのコンフィギュレーション変更を VLAN データベースに適用し、データベース コンフィギュレーション番号を増分し、管理ドメイン全体にこれを伝播し、特権 EXEC モードに戻ります。
- **no**：コマンドを無効にするか、デフォルトに設定します。指定できる値は **vlan** および **vtp** です。
- **reset**：VLAN データベースに加える予定の変更を破棄し、設定する予定のデータベースをスイッチ上で実施されている VLAN データベースにリセットし、VLAN コンフィギュレーション モードを継続します。
- **show**：VLAN データベース情報を表示します。
- **show changes** [*vlan-id*]：すべての標準範囲 VLAN ID（1 ～ 1005）または指定された VLAN ID（1 ～ 1005）に関して、スイッチ上の VLAN データベースと設定する予定の VLAN データベース間の相違を表示します。
- **show current** [*vlan-id*]：スイッチ上または選択された VLAN（1 ～ 1005）上の VLAN データベースを表示します。
- **show proposed** [*vlan-id*]：設定する予定の VLAN データベースを表示するか、または設定する予定のデータベースから選択した VLAN（1 ～ 1005）を表示します。設定しようとしている VLAN データベースは、**exit** または **apply** VLAN コンフィギュレーション コマンドを使用するまで実行コンフィギュレーションではありません。

show vlan 特権 EXEC コマンドを入力すると、VLAN データベース変更が行われたのか、それとも打ち切られたのかを確認できます。出力は、**show** VLAN データベース コンフィギュレーション コマンドの出力とは異なります。

例

次の例では、特権 EXEC コマンド モードから VLAN コンフィギュレーション モードを開始して、VLAN データベース情報を表示する方法を示します。

```
Switch# vlan database
Switch(vlan)# show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
```

```
    MTU: 1500

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

<output truncated>
```

次の例では、**show changes** コマンドの出力を示します。

```
Switch(vlan)# show changes

DELETED:
  VLAN ISL Id: 4
    Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

次の例では、現在のデータベースの VLAN 7 と設定しようとしているデータベースとの相違を表示する方法を示します。

```
Switch(vlan)# show changes 7

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

次の例では、**show current 20** コマンドの出力を示します。現在のデータベースの VLAN 20 だけが表示されます。

```
Switch(vlan)# show current 20
VLAN ISL Id: 20
    Name: VLAN0020
    Media Type: Ethernet
    VLAN 802.10 Id: 100020
    State: Operational
    MTU: 1500
```

関連コマンド

コマンド	説明
show vlan	管理ドメイン内のすべての設定された VLAN のパラメータを表示します。
shutdown vlan	指定された VLAN でローカル トラフィックをシャットダウン（停止）します。
vlan（グローバル コンフィギュレーション）	標準範囲および拡張範囲 VLAN を設定するための config-vlan モードを開始します。

vmps reconfirm（特権 EXEC）

ただちに VQP クエリーを送信して VMPS でのすべてのダイナミック VLAN 割り当てを再確認するには、**vmps reconfirm** 特権 EXEC コマンドを使用します。

vmps reconfirm

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトは定義されていません。

コマンド モード

特権 EXEC

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、VQP クエリーを VMPS にただちに送信する方法を示します。

```
Switch# vmps reconfirm
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Reconfirmation Status セクションの VMPS Action 列を調べます。**show vmps** コマンドは、再確認タイマー切れの結果または **vmps reconfirm** コマンドの入力のいずれかにより最後に割り当てが再確認された結果を表示します。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。
vmps reconfirm（グローバル コンフィギュレーション）	VQP クライアントの再確認間隔を変更します。

vmps reconfirm（グローバル コンフィギュレーション）

VLAN Query Protocol（VQP）クライアントの再確認の間隔を変更するには、**vmps reconfirm** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vmps reconfirm *interval*

no vmps reconfirm

シンタックスの説明

interval	ダイナミック VLAN 割り当てを再確認するための VLAN メンバシップ ポリシー サーバ（VMPS）への VQP クライアント クエリーの再確認間隔。指定できる範囲は 1 ～ 120 分です。

デフォルト

デフォルトの再確認間隔は 60 分です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、VQP クライアントが 20 分ごとにダイナミック VLAN エントリを再確認するように設定する方法を示します。

```
Switch(config)# vmps reconfirm 20
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Reconfirm Interval 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。
vmps reconfirm（特権 EXEC）	VQP クエリーを送信して、VMPS でのすべてのダイナミック VLAN 割り当てを再確認します。

vmps retry

VLAN Query Protocol（VQP）クライアントに関してサーバごとの再試行回数を設定するには、**vmps retry** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vmps retry *count*

no vmps retry

シンタックスの説明

count	リストの次のサーバに照会する前にクライアントが VLAN メンバシップ ポリシー サーバ（VMPS）との通信を試行する回数。指定できる範囲は 1 ～ 10 です。

デフォルト

デフォルトの再試行回数は 3 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

例

次の例では、再試行回数を 7 に設定する方法を示します。

```
Switch(config)# vmps retry 7
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、Server Retry Count 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。

vmps server

プライマリ VMPS と 3 つまでのセカンダリ サーバを設定するには、**vmps server** グローバル コンフィギュレーション コマンドを使用します。VMPS サーバを削除するには、このコマンドの **no** 形式を使用します。

vmps server *ipaddress* [**primary**]

no vmps server [*ipaddress*]

シンタックスの説明

ipaddress	プライマリまたはセカンダリ VMPS サーバの IP アドレスまたはホスト名。ホスト名を指定する場合には、Domain Name System（DNS; ドメイン ネーム システム）サーバが設定されている必要があります。
primary	（任意）プライマリとセカンダリのどちらの VMPS サーバを設定するのかを決定します。

デフォルト

プライマリまたはセカンダリ VMPS サーバは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

primary が入力されているかどうかにかかわらず、最初に入力されたサーバは自動的にプライマリ サーバとして選択されます、最初のサーバ アドレスは、次のコマンドで **primary** を使用することにより無効にすることができます。

クラスタ コンフィギュレーションのメンバー スイッチに IP アドレスがない場合、クラスタはそのメンバー スイッチに設定された VMPS サーバを使用しません。その代わり、クラスタはコマンド スイッチの VMPS サーバを使用し、コマンド スイッチは VMPS 要求のプロキシとなります。VMPS サーバは、クラスタを単一スイッチとして扱い、コマンド スイッチの IP アドレスを使用して要求に応答します。

ipaddress を指定せずに **no** 形式を使用すると、すべての設定されたサーバが削除されます。ダイナミック アクセス ポートが存在するときにすべてのサーバを削除すると、スイッチは、VMPS に照会できないため、これらのポートの新しい送信元からのパケットを転送できません。

例

次の例では、IP アドレス 191.10.49.20 をプライマリ VMPS サーバとして設定する方法を示します。IP アドレス 191.10.49.21 および 191.10.49.22 のサーバは、セカンダリ サーバとして設定されます。

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

次の例では、IP アドレス 191.10.49.21 のサーバを削除する方法を示します。

```
Switch(config)# no vmps server 191.10.49.21
```

設定を確認するには、**show vmps** 特権 EXEC コマンドを入力して、VMPS Domain Server 列を調べます。

関連コマンド

コマンド	説明
show vmps	VQP および VMPS 情報を表示します。

vtp（グローバル コンフィギュレーション）

VTP 設定の特性を設定または修正するには、**vtp** グローバル コンフィギュレーション コマンドを使用します。設定を削除したり、デフォルト設定に戻したりする場合は、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** | **password** | **pruning** | **version**}

シンタックスの説明

domain *domain-name*	VTP ドメイン名をスイッチの VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file *filename*	VTP VLAN 設定が保存されている Cisco IOS ファイル システム ファイルを指定します。
interface *name*	このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。
only	（任意）VTP IP アップデータとしてこのインターフェイスの IP アドレスのみ使用します。
mode	VTP 装置モードをクライアント、サーバ、または透過型に指定します。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信できますが、VLAN 設定を保存する十分な不揮発性メモリを持ちません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信します。スイッチで VLAN を設定できます。スイッチは、再起動後不揮発性メモリから現在の VTP データベースのすべての VLAN 情報を回復できます。
transparent	スイッチを VTP 透過モードにします。VTP 透過モードのスイッチは VTP がディセーブルになっており、アドバタイズを送信したり、他の装置が送信したアドバタイズから学習したりしません。また、ネットワーク内の他の装置の VLAN 設定に影響を与えることはできません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。 VTP モードが透過型である場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。
password *password*	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
pruning	スイッチ上で VTP プルーニングをイネーブルに設定します。
version *number*	VTP バージョンをバージョン 1 またはバージョン 2 に設定します。

デフォルト

デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードです。

ドメイン名またはパスワードは定義されていません。

パスワードは設定されていません。

プルーニングはディセーブルです。

デフォルトのバージョンはバージョン 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VTP モード、VTP ドメイン名、および VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- VLAN データベースとコンフィギュレーション ファイルの両方の VTP モードが透過型であり、VTP ドメイン名が一致する場合、VLAN データベースは無視されます。スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ VTP モードがサーバ モードの場合、またはスタートアップ VTP モードまたはドメイン名が VLAN データベースと一致しない場合、最初の 1005 の VTP および VLAN 設定は、VLAN データベース情報によって選択され、1005 を超える VLAN は、スイッチ コンフィギュレーション ファイルから設定されます。

新規データベースをロードするのに **vtp file** *filename* を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートに置かれます。非管理ドメイン ステートに置かれている間は、ローカル VLAN 設定に変更が生じてもスイッチは VTP アドバタイズを送信しません。スイッチは、トランキングを行っているポートで最初の VTP サマリー パケットを受信したあと、または **vtp domain** コマンドでドメイン名を設定したあとで、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信すると、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから出たあと、NVRAM をクリアしてソフトウェアをリロードするまで、スイッチがこのステートにもう一度入るように設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、スイッチを VTP サーバ モードに戻すことができます。
- **vtp mode server** コマンドは、スイッチがクライアント モードまたはトランスペアレント モードでない場合にエラーを戻さないことを除けば、**no vtp mode** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバのコンフィギュレーションをコピーします。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたは透過モードである場合、スイッチの設定は変更されません。
- 透過モードのスイッチは、VTP に参加しません。透過モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードにあるスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードは透過型に設定してください。
- 拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、そのコンフィギュレーションは許可されません。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかにかぎります。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードでは、大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチをパスワードが設定されていない状態に戻す場合は、このコマンドの **no vtp password** 形式を使用します。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ～ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2（v2）モード ステートのトグリングを行うと、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼動するよう設定する必要があります。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。

- トークンリング ブリッジ リレー機能（TrBRF）または Token Ring Concentrator Relay Function（TrCRF; トークンリング コンセントレータ リレー機能）VLAN メディア タイプを設定している場合は、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。

スイッチ コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

例

次の例では、VTP コンフィギュレーション メモリのファイル名を *vtpfilename* に変更する方法を示します。

```
Switch(config)# vtp file vtpfilename
```

次の例では、デバイス ストレージのファイル名をクリアする方法を示します。

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Switch(config)# vtp interface gigabitethernet
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(config)# vtp domain OurDomainName
```

次の例では、スイッチを VTP 透過モードにする方法を示します。

```
Switch(config)# vtp mode transparent
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(config)# vtp pruning
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Switch(config)# vtp version 2
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vtp status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
vtp（VLAN コンフィギュレーション）	VTP のドメイン名、パスワード、プルーニング、バージョンおよびモードを設定します。

vtp（VLAN コンフィギュレーション）

VTP の特性を設定するには、**vtp** VLAN コンフィギュレーション コマンドを使用します。VLAN コンフィギュレーション モードを開始する場合は、**vlan database** 特権 EXEC コマンドを入力します。デフォルト設定に戻したり、特性をディセーブルにしたり、パスワードを削除したりする場合は、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | {**server** | **client** | **transparent**}}

no vtp {**client** | **password** | **pruning** | **transparent** | **v2-mode**}

シンタックスの説明

domain *domain-name*	スイッチの VTP 管理ドメインを識別する VTP ドメイン名を、1 ～ 32 文字の ASCII 文字列を入力して設定します。ドメイン名では大文字と小文字が区別されます。
password *password*	VTP アドバタイズで送信され、受信 VTP アドバタイズを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
pruning	VTP 管理ドメインでプルーニングをイネーブルにします。VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
v2-mode	管理ドメインで VLAN トランキング プロトコル（VTP）バージョン 2 をイネーブルにします。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信できますが、VLAN 設定を保存する十分な不揮発性メモリを持ちません。スイッチで VLAN を設定することはできません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは、VTP がイネーブルになっており、アドバタイズを送信します。スイッチで VLAN を設定できます。スイッチは、再起動後不揮発性メモリから現在の VTP データベースのすべての VLAN 情報を回復できます。
transparent	スイッチを VTP 透過モードにします。VTP 透過モードのスイッチは VTP がディセーブルになっており、アドバタイズを送信したり、他の装置が送信したアドバタイズから学習したりしません。また、ネットワーク内の他の装置の VLAN 設定に影響を与えることはできません。スイッチは VTP アドバタイズを受信し、アドバタイズを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。

デフォルト

デフォルト モードはサーバ モードです。

ドメイン名は定義されていません。

パスワードは設定されていません。

プルーニングはディセーブルです。

VTP バージョン 2（v2 モード）はディセーブルです。

コマンド モード　VLAN コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(25)FX	このコマンドが追加されました。

使用上のガイドライン

VTP モードが透過型である場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを入力します。

VTP モードを設定するときには、次の注意事項に従ってください。

- スイッチを VTP サーバ モードに戻すには、このコマンドの **no vtp client** および **no vtp transparent** 形式を使用します。
- **vtp server** コマンドは、スイッチがクライアント モードまたはトランスペアレント モードでない場合にエラーを戻さないことを除けば、**no vtp client** または **no vtp transparent** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバのコンフィギュレーションをコピーします。クライアント モードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。受信スイッチがサーバ モードまたは透過モードである場合、スイッチの設定は変更されません。
- 透過モードのスイッチは、VTP に参加しません。透過モードのスイッチで VTP または VLAN 設定の変更を行った場合、変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードにあるスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 設定を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードは透過型に設定してください。
- 拡張範囲 VLAN がスイッチで設定され、VTP モードをサーバまたはクライアントに設定しようとした場合、エラー メッセージが表示され、その設定は許可されません。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかにかぎります。

（注）　VTP コンフィギュレーション モードの VTP 設定は、適用されたときに VLAN データベースに保存されます。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートに置かれます。非管理ドメイン ステートに置かれている間は、ローカル VLAN 設定に変更が生じてもスイッチは VTP アドバタイズを送信しません。スイッチは、トランキングを行っているポートで最初の VTP サマリー パケットを受信したあと、または **vtp domain** コマンドでドメイン名を設定したあとで、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから抜け出したあと、NVRAM をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードでは、大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチを非パスワード ステートに戻す場合は、このコマンドの **no vtp password** 形式を使用します。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP サーバでプルーニングをイネーブルにすると、プルーニングは管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョン 2（v2 モード）をイネーブルにする場合には、次の注意事項に従ってください。

- バージョン 2（v2 モード）ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼動するよう設定する必要があります（**no vtp v2-mode**）。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、またはトークンリング ブリッジ リレー機能（TrBRF）やトークンリング コンセントレータ リレー機能（TrCRF）VLAN メディア タイプを設定している場合には、VTP バージョン 2（**v2-mode**）をイネーブルにしてください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、VTP バージョン 1 を使用してください。

例

次の例では、スイッチを VTP 透過モードにする方法を示します。

```
Switch(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(vlan)# vtp domain OurDomainName
Changing VTP domain name from cisco to OurDomainName
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(vlan)# vtp password private
Setting device VLAN database password to private.
```

次の例では、設定しようとしている新規 VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(vlan)# vtp pruning
Pruning switched ON
```

次の例では、設定しようとしている新規 VLAN データベースで v2 モードをイネーブルにする方法を示します。

```
Switch(vlan)# vtp v2-mode
V2 mode enabled.
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show vtp status	スイッチの VTP 統計情報および VTP 管理ドメイン ステータスの一般情報を表示します。
switchport trunk pruning	トランキング モードのポートの VLAN プルーニング適格リストを設定します。
vtp（グローバル コンフィギュレーション）	VTP ファイル名、インターフェイス、ドメイン名、およびモードを設定します。