

トラブルシューティング：トランスペアレントブリッジング環境

目次

[目的](#)

[トランスペアレントブリッジングテクノロジーの基礎](#)

[ブリッジングループ](#)

[スパニングツリーアルゴリズム](#)

[フレーム形式](#)

[メッセージフィールド](#)

[さまざまなIOSブリッジング技術](#)

[トランスペアレントブリッジングのトラブルシューティング](#)

[トランスペアレントブリッジング：接続できない](#)

[トランスペアレントブリッジング：不安定なスパニングツリー](#)

[トランスペアレントブリッジング：セッションが突然終了する](#)

[トランスペアレントブリッジング：ループとブロードキャストストームが発生する](#)

[Cisco TAC チームへのお問い合わせの前に](#)

[その他の情報源](#)

[関連情報](#)

目的

トランスペアレントブリッジは Digital Equipment Corporation (DEC) 社が 1980 年代初頭に初めて開発したもので、現在では、イーサネット/IEEE 802.3 ネットワークで一般的に使用されています。

- この章では最初に、トランスペアレントブリッジを、スパニングツリープロトコルを実装するラーニングブリッジとして定義します。また、スパニングツリープロトコルの詳細についても説明します。
- トランスペアレントブリッジを実装するシスコのデバイスは、もともと Cisco IOS® ソフトウェアが動作するルータと特定のソフトウェアが動作する Catalyst スイッチという 2 つのカテゴリに分類されていました。ただし、現在では、この分類は該当せず、多数の Catalyst 製品が IOS ベースになっています。この章では、IOS デバイスで使用できるさまざまなブリッジング技術を紹介します。Catalyst ソフトウェア固有の設定とトラブルシューティングについては、LAN スイッチングの章を参照してください。
- 最後に、トランスペアレントブリッジングネットワークで発生しやすい潜在的な問題の症状別に、トラブルシューティングの手順を紹介します。

[トランスペアレントブリッジングテクノロジーの基礎](#)

トランスペアレントブリッジという名称は、その存在と動作がネットワークに対してトランスペアレント（透過的）であることに由来しています。トランスペアレントブリッジは起動時に、接続されているすべてのネットワークからの着信フレームの発信元アドレスを解析して、ネットワークのトポロジを学習します。たとえば、ホスト A からライン 1 に到着するフレームが検出されると、ブリッジはライン 1 に接続されたネットワーク経由でホスト A に到達可能であると判断します。このプロセスを介して、トランスペアレントブリッジは、表 20-1 のような内部ブリッジングテーブルを構築します。

表 20-1：トランスペアレントブリッジングテーブル

ホスト アドレス	ネットワーク番号
0000.0000.0001	1
0000.b07e.ee0e	7
?	-
0050.50e1.9b80	4
0060.b0d9.2e3d	2
0000.0c8c.7088	1
?	-

ブリッジは、ブリッジングテーブルに基づいてトラフィック転送を行います。ブリッジインターフェイスの一方でフレームが受信されると、ブリッジは内部テーブルでそのフレームの宛先アドレスを検索します。その内部テーブルで、宛先アドレスとブリッジ（フレーム受信先とは別のブリッジ）のいずれかのポートの間でマッピングされている場合、フレームはそこで指定されているポートに転送されます。マッピングが見つからない場合、そのフレームはすべての発信ポートにフラッディングされます。また、ブロードキャストとマルチキャストも同じようにフラッディングされます。

トランスペアレントブリッジでは、セグメント内のトラフィックが適切に切り分けられるので、各セグメントで検出されるトラフィックは減少します。これにより、通常はネットワークの応答時間が改善されます。どの程度トラフィックが削減され、応答時間が改善されるかは、セグメント間トラフィック量（総トラフィック量に対する割合）および、ブロードキャストトラフィックとマルチキャストトラフィックの量によって異なります。

ブリッジングループ

インターネットワークの 2 つの LAN 間にブリッジと LAN の複数のパスがある場合、ブリッジ間のプロトコルがないと、トランスペアレントブリッジアルゴリズムは失敗します。図 20-1 は、このようなブリッジングループを示したものです。

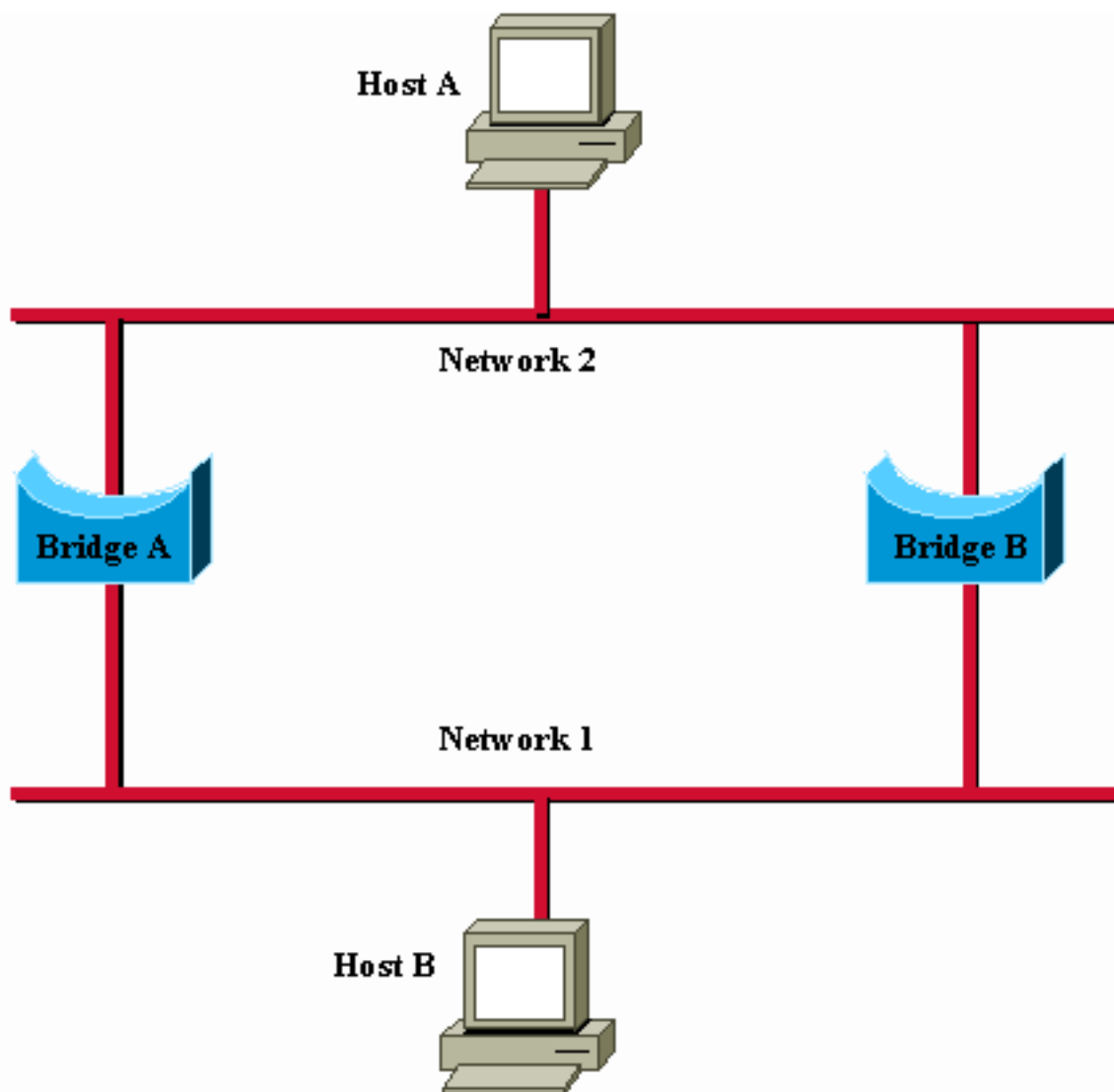


図 20-1：トランスペアレントブリッジング環境での不正確な転送と学習

ホスト A からホスト B にフレームが送信されるとします。両方のブリッジがフレームを受信し、ホスト A がネットワーク 2 上にあることは適切に判断されます。しかし、ホスト B がホスト A からのフレームのコピーを 2 つ受信すると、両方のブリッジが再度ネットワーク 1 のインターフェイスでフレームを受信してしまいます。これは、すべてのホストがブロードキャスト LAN 上のすべてのメッセージを受信するためです。また、場合によっては、ブリッジが内部テーブルを書き換え、ホスト A がネットワーク 1 に存在するものと示すことがあります。この場合、テーブルでは宛先 (ホスト A) がフレームの発信元と同じネットワークセグメント上に存在することになっているため、ホスト B がホスト A のフレームに応答する際に、両方のブリッジが応答を受信した後で廃棄してしまいます。

上記のような接続に関する基本的な問題のほかに、ネットワーク上でのループを伴うブロードキャストメッセージの増加が、重大なネットワークの問題として潜んでいます。たとえば、図 20-1 の例で、ホスト A の最初のフレームがブロードキャストだとします。この場合、両方のブリッジが無限にフレームを転送することになり、使用できるすべてのネットワーク帯域幅が消費されるため、両方のセグメントで他のパケットの伝送がブロックされてしまいます。

図 20-1 に示すようなループを伴うトポロジは、有用な場合もありますが、問題を引き起こす可能性もあります。ループがあるということは、インターネットワークを介した複数のパスが存在することを意味します。発信元から宛先への複数のパスがあるネットワークには、トポロジに柔軟性があり、これによってネットワーク全体の耐障害性が向上します

スパニング ツリー アルゴリズム

スパニング ツリー アルゴリズム (STA) は、ループの利点を維持しながら、その問題を取り除くために、イーサネットの主要ベンダーであった DEC 社で開発されました。DEC 社のアルゴリズムはその後、IEEE 802 委員会で改訂され、IEEE 802.1d 仕様として公開されました。この DEC 社のアルゴリズムと IEEE 802.1d のアルゴリズムは同一ではなく、互換性はありません。

STA とは、ループを形成するブリッジ ポートがある場合に、そのポートをスタンバイ (ブロッキング) 状態にすることでループの発生を防ぐネットワーク トポロジのサブセットのことです。プライマリ リンクに障害が発生するとブリッジ ポートのブロッキングが有効になり、インターネットワークを介して新しいパスを提供します。

STA では、ループの発生を防ぐネットワーク トポロジのサブセットの構築のベースとして、グラフ理論を使用しています。グラフ理論では、「複数のノードとエッジがノードのペアを接続する連結グラフには、ループを含まずグラフの接続性を維持するエッジのスパニング ツリーが存在する」とされています。

図 20-2 は、STA がどのようにループを解消するのかを示したものです。STA では、各ブリッジに一意の ID を割り当てる必要があります。一般的に、この ID はブリッジの MAC アドレスの 1 つに優先度を付け加えたものです。また、すべてのブリッジの各ポートには、該当するブリッジ内で一意の ID も割り当てられます (通常はポート自身の MAC アドレス)。最後に、各ブリッジポートにはパスコストが関連付けられています。パスコストは、そのポートを介して LAN にフレームを送信するコストを表したものです。図 20-2 では、各ブリッジから出ている回線にパスコストが記入されています。パスコストは通常デフォルト値になっていますが、ネットワーク管理者が手動で割り当てることもできます。

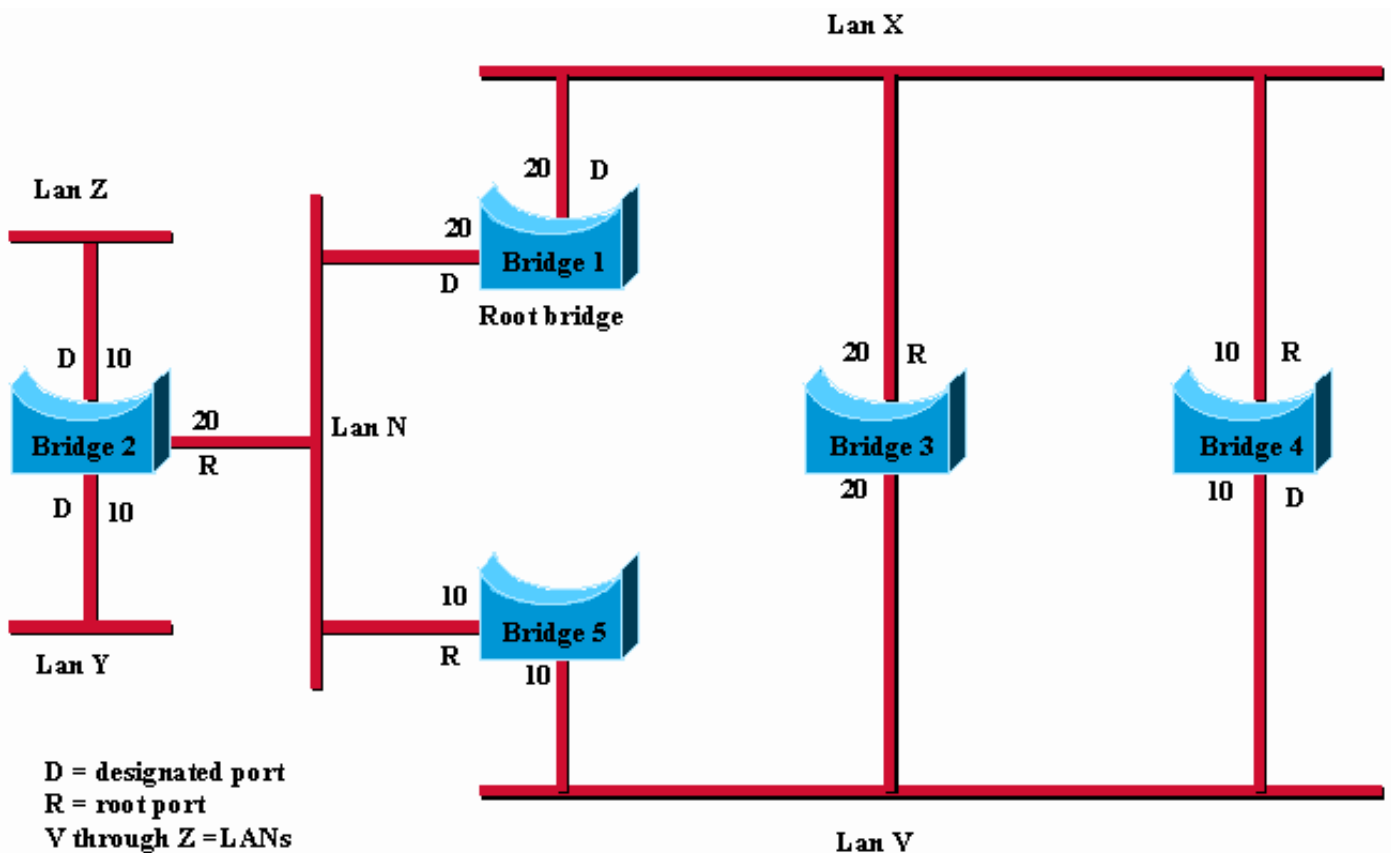


図 20-2: トランスペアレント ブリッジ ネットワーク (STA 実装前)

スパニング ツリーの計算で最初に行われるのは、ルートブリッジの選択です。ルートブリッジ

とは、ブリッジ ID の値が最も低いブリッジです。図 20-2 では、ブリッジ 1 がルートブリッジとなります。次に、他のすべてのブリッジのルートポートが決定されます。ブリッジのルートポートは、ルートブリッジが最小の集約パスコストで到着できるポートです。ルートブリッジへの最小の集約パスコストの値はルートパスコストと呼ばれます。

最後に、代表ブリッジとその代表ポートが決定されます。代表ブリッジとは、各 LAN 上のブリッジの中で、最低ルートパスコストを提供するブリッジのことです。LAN の代表ブリッジだけが、その LAN へのフレーム転送および LAN からのフレーム転送を許可されています。LAN の代表ポートとは、代表ブリッジに接続するポートのことです。

場合によっては、複数のブリッジが同じルートパスコストを持つことがあります。たとえば、図 20-2 で、ブリッジ 4 および 5 はブリッジ ID 再度使用されます、代表ブリッジを判別する今回、10 のパスコストでブリッジ 1 (ルートブリッジ) にこの場合達することができます。ブリッジ 5 の LAN V ポートではなく、ブリッジ 4 の LAN V ポートが選択されます。

このプロセスを使用して、各 LAN に直接接続されたブリッジが 1 つを除いて排除されることで、複数の LAN にまたがるループがなくなります。STA でも、複数の LAN にまたがるループが排除されますが、接続性は保たれています。図 20-3 は、図 20-2 で示されたネットワークに STA を適用した結果を示したものです。図 20-2 ではツリートポロジがより明確に示されています。この図を図 20-3 と比較すると、STA が LAN V へのブリッジ 3 とブリッジ 5 両方のポートをスタンバイモードにしていることがわかります。

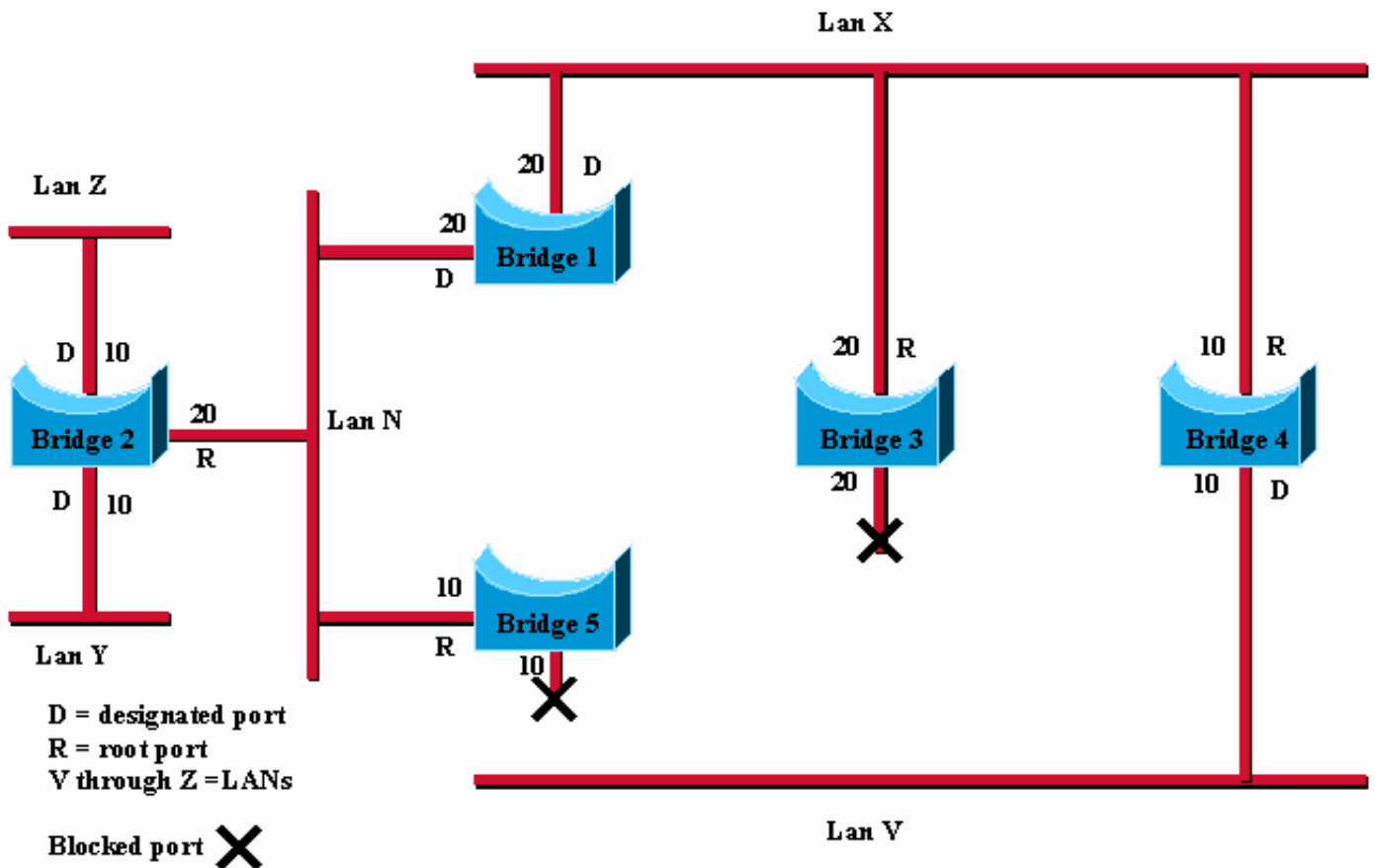


図 20-3: トランスペアレントブリッジネットワーク (STA 実装後)

スパニングツリーの計算は、ブリッジに電源が投入されたとき、およびトポロジの変更が検出されたときに行われます。この計算にはスパニングツリーブリッジ間の通信が必要で、設定メッセージ (ブリッジプロトコルデータユニットとも呼ばれる) を介して行われます。設定メッセージには、ルートと想定されるブリッジを識別する情報 (ルート ID)、および送信ブリッジからルートブリッジへの距離 (ルートパスコスト) が含まれています。設定メッセージには、送信

ブリッジのブリッジとポート ID、およびその設定メッセージ内に含まれる情報の経過時間も含まれています。

ブリッジ同士は、設定メッセージを一定の間隔（通常は 1 ~ 4 秒）で交換します。ブリッジに障害が発生した場合（トポロジ変更が発生した場合）、隣接したブリッジでは設定メッセージの欠落をすぐに検出し、スパニング ツリーの再計算を開始します。

トランスペアレント ブリッジ トポロジはすべてローカルに決定されます。設定メッセージは、隣接したブリッジ間で交換されます。ネットワーク トポロジや管理に関して、集中的な権限は存在しません。

フレーム形式

トランスペアレント ブリッジでは、設定メッセージとトポロジ変更メッセージを交換します。設定メッセージをブリッジ間で交換することで、ネットワーク トポロジが確立されます。トポロジの変更が検出されるとトポロジ変更メッセージが送信され、STA を再実行する必要があることが通知されます。

表 20-2 では IEEE 802.1d の設定メッセージの形式を示しています。

表 20-2：トランスペアレント ブリッジの設定

プロトコル ID	バージョン	メッセージタイプ	フラグ	ルート ID	ルートパスコスト	ブリッジ ID	ポート ID	メッセージの経過時間	最大経過時間	Hello タイム	転送遅延
2 バイト	1 バイト	1 バイト	1 バイト	8 bytes	4 バイト	8 bytes	2 バイト	2 バイト	2 バイト	2 バイト	2 バイト

メッセージ フィールド

トランスペアレント ブリッジ設定メッセージは 35 バイトで構成されています。メッセージ フィールドは次のとおりです。

- プロトコル ID バージョン：値は 0 です。
- バージョン バージョン：値は 0 です。
- メッセージ タイプ バージョン：値は 0 です。
- フラグ：1 バイトのフィールドですが、使用されるのは最初の 2 ビットだけです。トポロジ変更 (TC) ビットで、トポロジ変更が通知されます。トポロジ変更確認応答 (TCA) ビットをセットして、TC ビットがセットされた設定メッセージの受信を通知します。
- ルート ID：2 バイトの優先度の後に 6 バイトの ID を示してルート ブリッジを識別します。
- ルートパスコスト：設定メッセージを送信するブリッジからルートブリッジまでのパスコストです。

- ブリッジ ID：メッセージを送信するブリッジの優先度と ID を識別します。
- ポート ID：設定メッセージの送信元ポートを識別します。このフィールドにより、複数の接続ブリッジで形成されたループの検出と処理が可能になります。
- メッセージの経過時間：現在の設定メッセージの基になっている設定メッセージをルートから送信してから経過した時間を示します。
- 最大経過時間：現在の設定メッセージを消去するタイミングを示します。
- Hello タイム：ルートブリッジ設定メッセージの送信間隔です。
- 転送遅延：トポロジの変更から、新しいステートに遷移するまでブリッジが待機する時間です。ブリッジのステート遷移が早すぎると、すべてのネットワークリンクでステート変更の準備ができていないため、ループが発生する場合があります。

トポロジ変更メッセージの形式は、トランスペアレントブリッジ設定メッセージの形式に類似していますが、最初の 4 バイトだけで構成されている点が異なります。メッセージフィールドは次のとおりです。

- プロトコル ID バージョン：値は 0 です。
- バージョン バージョン：値は 0 です。
- メッセージタイプ 値 128 を示します。

さまざまな IOS ブリッジング技術

シスコのルータでは、デフォルト動作、同時ルーティングおよびブリッジング (CRB)、Integrated Routing and Bridging (IRB) という 3 種類のブリッジング実装方法が採用されています。

デフォルト動作

IRB および CRB が使用可能になる前は、プラットフォームベースだけでプロトコルのブリッジングまたルーティングが可能でした。つまり、たとえば `ip route` コマンドが使用された場合は、すべてのインターフェイスで IP ルーティングが行われていました。この場合、IP はルータのどのインターフェイスでもブリッジングを行うことができません。

同時ルーティングおよびブリッジング (CRB)

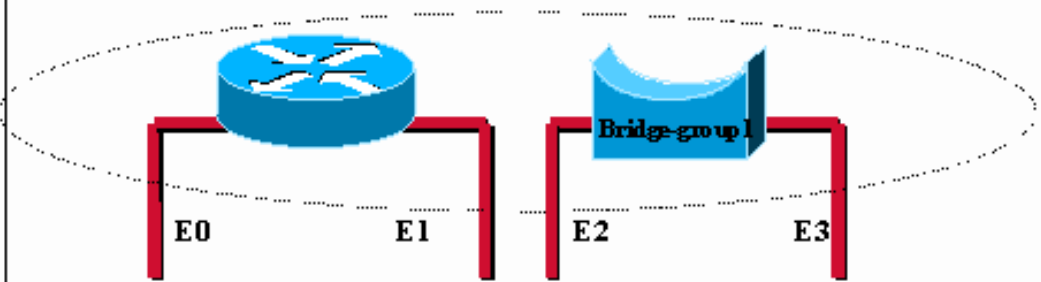
CRB では、プロトコルをブリッジングするかルーティングするかをインターフェイスベースで決定できます。つまり、あるインターフェイスで特定のプロトコルのルーティングをし、同じルータ内のブリッジグループインターフェイスで同じプロトコルのブリッジングをすることが可能です。そのルータは特定のプロトコルに対してルータとブリッジを兼ねることができます。しかし、ルーティングが定義されたインターフェイスとブリッジグループインターフェイスとの間には、通信はありません。

次の例では、特定のプロトコルに関して、単一のルータが論理的には独立した複数のデバイスとして機能できることを示します。独立したデバイスとは、1 つのルータと 1 つ以上のブリッジです。


```

bridge crb
interface e0
    ip address X
interface e1
    ip address Y
interface e2
    bridge-group 1
interface e3
    bridge-group 1
bridge 1 protocol ieee

```



In this configuration, for the IP protocol, the Cisco device is acting like a router for interface e0 and e1 and is acting like a bridge for interface e2 and e3. Note that there is no communication possible between the two functions (a host connected on e0 would never be able to reach a host connected on e2 through the router with this configuration).

図 20-4: 同時ルーティングおよびブリッジング (CRB)

Integrated Routing and Bridging (IRB)

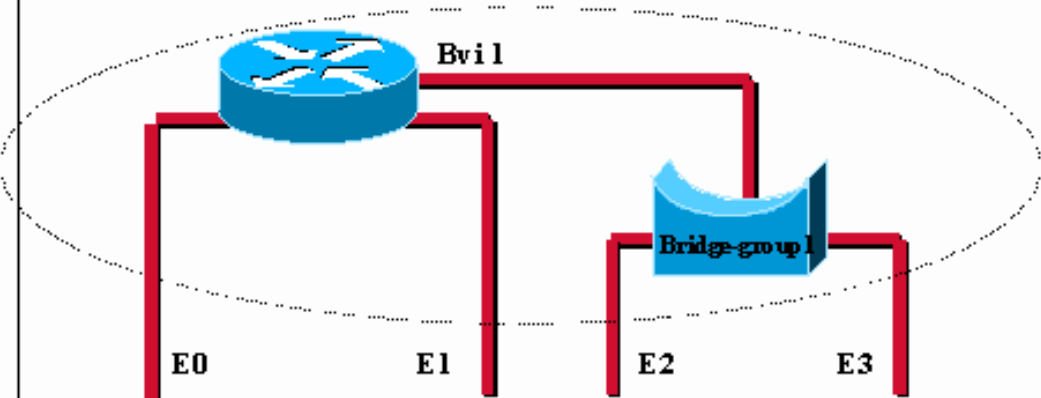
IRB は、ブリッジ グループ仮想インターフェイス (BVI) と呼ばれる概念を使用して、ブリッジグループとルーテッド インターフェイス間でのルーティング機能を提供します。ブリッジングはデータ リンク層で実行され、ルーティングはネットワーク層で実行されるため、ブリッジングとルーティングはプロトコル設定モデルが異なります。たとえば IP では、ブリッジグループ インターフェイスは同じネットワークに属していて、集合的な IP ネットワーク アドレスが付いていますが、個々のルーテッド インターフェイスは、独自の IP ネットワーク アドレスが付いた固有のネットワークを表しています。

BVI の概念は、これらのインターフェイスで任意のプロトコルでのパケット交換を可能にするために作成されたものです。概念的には、次の例に示されているように、シスコのルータは 1 つ以上のブリッジ グループに接続されたルータのように動作します。

```

bridge irb
interface e0
    ip address X
interface e1
    ip address Y
interface e2
    bridge-group 1
interface e3
    bridge-group 1
interface bvi 1
    ip address Z
bridge 1 protocol ieee

```

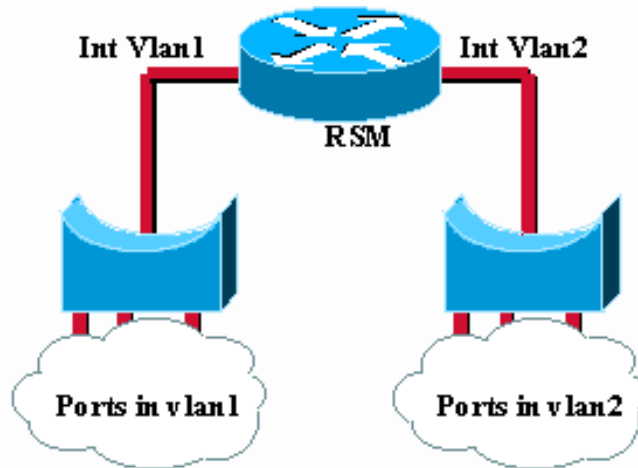


The bridge group virtual interface brings routing to bridge-group 1. One can assign an Ip address to the whole bridge-group and routed communication is now possible between a host connected to E0 and a host connected to E2 for instance.

図 20-5: Integrated Routing and Bridging (IRB)

BVI は、通常のルーテッド インターフェイスのように動作するルータ内の仮想インターフェイスです。BVI は、ルータ内のルーテッド インターフェイスに対応するブリッジ グループとなっています。BVI のインターフェイス番号は、この仮想インターフェイスで代表されたブリッジ グループの番号になります。この番号が BVI とブリッジ グループ間のリンクになります。

次の例は、Catalyst スイッチのルート スイッチ モジュール (RSM) に BVI が適用される仕組みを示したものです。



The IRB concept is also used (but hidden) on the Catalyst Route Switch Module (RSM). The vlan interfaces are in fact virtual interfaces connecting different bridge groups (the vlans).

図 20-6: Catalyst スイッチでのルート スイッチ モジュール (RSM)

トランスペアレント ブリッジングのトラブルシューティング

このセクションでは、トランスペアレント ブリッジング インターネットワークでの接続性の問題に関するトラブルシューティング情報を紹介します。トランスペアレント ブリッジングの特定の症状、それぞれの症状を引き起こす可能性が高い問題点、そのような問題の解決策について説明します。

注: ソースルート ブリッジング (SRB)、トランスレーショナル ブリッジング、ソースルート トランスペアレント ブリッジング (SRT) に関連する問題は、第 10 章「IBM 製品のトラブルシューティング」で取り上げています。

ブリッジ型ネットワークのトラブルシューティングを効率的に実施するためには、その設計 (特にスパニング ツリーが使用される場合) についての基本的な知識が必要です。

次のものを用意しておいてください。

- ブリッジ型ネットワークのトポロジ マップ
- ルート ブリッジのロケーション
- 冗長リンク (およびブロックされているポート) の位置

接続性の問題をトラブルシューティングする際には、ホスト数を最少にします。1つのクライアントと1つのサーバだけにすることが理想です。

次のセクションでは、トランスペアレント ブリッジ型ネットワークで最も一般的に発生するネットワークの問題について説明します。

- [トランスペアレントブリッジング：接続できない](#)
- [トランスペアレントブリッジング：不安定なスパニングツリー](#)
- [トランスペアレントブリッジング：セッションが突然終了する](#)
- [トランスペアレントブリッジング：ループとブロードキャストストームが発生する](#)

[トランスペアレントブリッジング：接続できない](#)

症状：クライアントが、トランスペアレントブリッジ型ネットワーク経由でホストに接続できない。

表 20-3 はこの現象を引き起こす場合がある概説し、ソリューションを提案したものです問題を。

表 20-3：トランスペアレントブリッジング：接続できない

考えられる原因	推奨される対策
ハードウェアまたはメディアの問題	<ol style="list-style-type: none"> 1. <code>show bridge EXEC</code> コマンドを使用して、接続性の問題があるかどうかを確認します。問題がある場合は、ブリッジングテーブルに MAC[1] アドレスが出力されません。 2. <code>show interfaces EXEC</code> コマンドを使用して、インターフェイスとラインプロトコルがアップ状態であるかどうかを判別します。 3. インターフェイスがダウンしている場合は、ハードウェアまたはメディアの問題をトラブルシューティングします。第 3 章「ハードウェアとブートの問題のトラブルシューティング」を参照してください。 4. ラインプロトコルがダウンしている場合は、そのインターフェイスとネットワークの間の物理的な接続を確認します。確実に接続されていることと、ケーブルが損傷していないことを確認してください。 <p>ラインプロトコルがアップ状態であるにもかかわらず、入出力パケットカウンタが増加していない場合は、メディアとホストの接続性を確認します。ご使用のネットワークで使用されているメディアタイプについて説明しているメディアトラブルシューティングの章を参照してください。</p>
ホストがダウンしている	<ol style="list-style-type: none"> 1. ブリッジで <code>show bridge EXEC</code> コマンドを使用して、接続されたエンドノードの MAC アドレスがブリッジングテーブルに入っていることを確認します。ブリッジングテーブルはホストの

	<p>発信元および宛先 MAC アドレスで構成されており、発信元あるいは宛先からのパケットがブリッジを通過すると、値が入ります。</p> <ol style="list-style-type: none"> 2. 予期されるエンドノードが見つからない場合は、そのノードのステータスをチェックして、接続されていることと適切な設定になっていることを確認します。 3. 必要に応じてエンドノードの再初期化と再設定を行い、show bridge コマンドを使用して、ブリッジング テーブルを再確認してください。
ブリッジングパスが壊れている	<ol style="list-style-type: none"> 1. エンドノード間でパケットが辿るパスを特定します。このパス上にルータがある場合、ノード 1 からルータ、およびルータから ノード 2 という 2 つの部分に分けてトラブルシューティングを実施します。 2. パス上の各ブリッジに接続して、エンドノード間のパスで使用されているポートのステータスを確認します (上記の「ハードウェアまたはメディアの問題」の項目で説明) 。 3. show bridge コマンドを使用して、ノードの MAC アドレスが適切なポートで学習されていることを確認します。学習されていない場合、スパニング ツリー トポロジが不安定になる可能性があります。表 20-2 「トランスペアレントブリッジング：不安定なスパニング ツリー」を参照してください。 4. show span コマンドでポートの状態を確認します。エンドノード間でトラフィックを伝送するポートがフォワーディング ステートになっていない場合は、ツリーのトポロジが予期せず変更されている可能性があります。表 20-4 「トランスペアレントブリッジング：不安定なスパニング ツリー」を参照してください。
ブリッジフィルタの設定が不適切	<ol style="list-style-type: none"> 1. show running-config 特権 EXEC コマンドを使用して、ブリッジ フィルタが設定されているかどうかを判別します。 2. 問題が疑われるインターフェイスのブリッジ フィルタを無効にして、接続性

	<p>が回復するかどうかを確認します。</p> <ol style="list-style-type: none"> 3. 接続性が回復しない場合、問題はフィルタではありません。フィルタを無効にすると接続性が回復する場合は、1つまたは複数の不良フィルタが問題の原因です。 4. フィルタが複数存在するか、複数のステートメントがあるアクセスリストを使用したフィルタが存在する場合は、問題のフィルタを特定するために、各フィルタを1つずつ適用し、入出力用の LSAP[2] および TYPE フィルタの設定を確認します。これらは、異なるプロトコルのブロッキングを行うために、同時に使用できません。たとえば、LSAP (F0F0) を NetBIOS のブロッキングに使用し、TYPE (6004) を ローカル エリア トランスポートのブロッキングに使用できます。 5. トラフィックをブロックする任意のフィルタまたはアクセスリストを修正します。すべてのフィルタを有効にしても接続状態を維持できるまで、フィルタのテストを続行してください。
<p>入力キューと出力キューがいっぱいになっている</p>	<p>過剰なマルチキャストまたはブロードキャストトラフィックが原因で、入力キューと出力キューがオーバーフローし、その結果パケットが廃棄される可能性があります。</p> <ol style="list-style-type: none"> 1. show interfaces コマンドを使用して、入出力の廃棄を探します。廃棄がある場合は、メディアに対して過剰なトラフィックがある可能性が示唆されています。入力キューの現在のパケットの数が現在の入力キュー サイズの 80 % を常に超えている場合、パケットレートに対応するために、入力キューのサイズを調整する必要があります。入力キューの現在のパケット数が入力キューのサイズに近づいているようには見えない場合でも、パケットのバーストによりキューがオーバーフローする可能性があります。 2. ブリッジング フィルタを実装して、接続されているネットワークでのブロードキャストとマルチキャストのトラフィックを削減するか、さらに多くのインターネットワーキング デバイスを使

	<p>用して、ネットワークをセグメント化します。</p> <p>3. 接続がシリアルリンクである場合は、帯域幅を増加させる、プライオリティキューイングを適用する、ホールドキューサイズを増加させる、システムバッファのサイズを変更するといった方法を試すことができます。詳細については、15章の「トラブルシューティング：シリアル回線の問題」を参照してください。</p>
--	---

[1]MAC = Media Access Control

[2]LSAP = Link Services Access Point

トランスペアレントブリッジング：不安定なスパニングツリー

症状：ホスト間の接続が一時的に途切れる。同時に複数のホストが影響を受けます。

表 20-4 はこの現象を引き起こす場合がある概説し、ソリューションを提案したものです問題を。

表 20-4：トランスペアレントブリッジング：不安定なスパニングツリー

考えられる原因	推奨される対策
リンクフラッピング	<p>1. <code>show span</code> コマンドを使用して、トポロジ変更の回数が増加し続けているかどうかを調べます。</p> <p>2. 増加している場合は、<code>show interface</code> コマンドを使用して、ブリッジ間のリンクを確認します。このコマンドを使用しても、2つのブリッジ間のリンクフラッピングを確認できない場合は、ブリッジで <code>debug spantree event</code> 特権 EXEC コマンドを使用します。</p> <p>これにより、スパニングツリーに関連するすべての変更が記録されます。安定したトポロジでは、何も記録されないはずですが、追跡するリンクは、ブリッジデバイスを接続しているリンクだけです。エンドステーションへのリンクでの遷移はネットワークに影響しません。</p>

	<p>注: デバッグの出力には、CPU プロセスで高い優先度が割り当てられるため、debug spantree event コマンドを使用すると、システムが使用できなくなる場合があります。このため、debug コマンドは、特定の問題のトラブルシューティングか、シスコのテクニカル サポート スタッフとのトラブルシューティング セッション中に限定して使用してください。さらに、ネットワークのトラフィック量が低い時間帯やユーザが少ない時間帯に debug コマンドを使用するのがベストです。このような期間にデバッグを行うことにより、debug コマンド処理によるオーバーヘッドの増大がシステムの使用に影響を及ぼす可能性が低くなります。</p>
<p>ルート ブリッジが変化し続ける/複数のブリッジがルートであることを主張する</p>	<ol style="list-style-type: none"> 1. 複数のブリッジで show span コマンドを使用し、ブリッジ型ネットワーク全体でルート ブリッジ情報に一貫性があることを確認します。 2. ルートであることを主張するブリッジが複数ある場合は、それぞれのブリッジで同じスパニング ツリー プロトコルを実行していることを確認します (表 20-6 の「スパニング ツリー アルゴリズムのミスマッチ」を参照)。 3. ルート ブリッジで bridge <group> priority <number> コマンドを使用して、目的のブリッジを強制的にルートにします。priority の値が低いほど、ブリッジがルートになる可能性が高くなります。 4. ネットワークの直径を確認します。標準的なスパニング ツリーの設定では、2 つのホスト間のブリッジ ホップは 7 以上になりません。

<p>Hello が交換されない</p>	<ol style="list-style-type: none"> ブリッジが相互に通信しているか確認します。ネットワークアナライザまたは <code>debug spantree tree</code> 特権 EXEC コマンドを使用して、スパニング ツリー hello フレームが交換されているか確認します。注：デバッグの出力には、CPU プロセスで高い優先度が割り当てられるため、<code>debug spantree event</code> コマンドを使用すると、システムが使用できなくなる場合があります。このため、<code>debug</code> コマンドは、特定の問題のトラブルシューティングか、シスコのテクニカル サポート スタッフとのトラブルシューティングセッション中に限定して使用してください。さらに、ネットワークのトラフィック量が低い時間帯やユーザが少ない時間帯に <code>debug</code> コマンドを使用するのがベストです。このような期間にデバッグを行うことにより、<code>debug</code> コマンド処理によるオーバーヘッドの増大がシステムの使用に影響を及ぼす可能性が低くなります。 hello が交換されていない場合は、ブリッジの物理的な接続とソフトウェア設定を確認します。
----------------------	--

トランスペアレントブリッジング：セッションが突然終了する

症状：トランスペアレントブリッジング環境で接続が確立しているのに、セッションが突然終了することがある。

表 20-5 はこの現象を引き起こす場合がある概説し、ソリューションを提案したものです問題を。

表 20-5：トランスペアレントブリッジング：セッションが突然終了する

<p>考え</p>	<p>推奨される対策</p>
-----------	----------------

<p>られる原因</p>	
<p>過剰な再送信</p>	<ol style="list-style-type: none"> 1. ネットワークアナライザを使用して、ホストの再送信を探します。 2. 低速のシリアル回線で再送信が検出された場合は、ホスト上の送信タイマーを増加させます。ホストの設定方法については、ベンダーのドキュメントを参照してください。シリアル回線のトラブルシューティングの情報については、第 15 章「トラブルシューティング：シリアル回線の問題」を参照してください。高速 LAN メディアで再送信が検出された場合は、送信されたパケットと受信されたパケットを順序どおりに確認するか、中継デバイス（ブリッジやスイッチなど）で廃棄されたパケットを確認します。LAN メディアのトラブルシューティングを適切に行います。詳細については、ご使用のネットワークで使用されているメディアタイプについて説明しているメディアトラブルシューティングの章を参照してください。 3. ネットワークアナライザを使用して、再送信数が減っているかどうかを判別します。
<p>シリアルリンクでの過剰な遅延</p>	<p>帯域幅を増加させる、プライオリティキューを適用する、ホールドキューサイズを増加させる、システムバッファのサイズを変更するといった方法を試すことができます。詳細については、15 章の「トラブルシューティング：シリアル回線の問題」を参照してください。</p>

トランスペアレントブリッジング：ループとブロードキャストストームが発生する

症状：トランスペアレントブリッジング環境で、パケットのループとブロードキャストストームが発生する。エンドステーションでは強制的に過剰な再送信が行われ、セッションのタイムアウトや破棄が発生する。

注：パケットループの原因は、通常、ネットワーク設計の問題か、ハードウェアの問題です。

表 20-6 では、この症状を引き起こす可能性のある問題の概要を示して、解決策を提案します。

ブリッジングループは、すべてのユーザに影響が出る可能性があるため、ブリッジ型ネットワークにおける最悪のシナリオです。緊急の場合は、ネットワーク内で冗長パスを形成しているすべてのインターフェイスを手動で無効にし、早急に接続を回復させることが最善策になります。ただし、この方法では、その後のブリッジングループの原因特定が非常に困難になります。可能であれば、事前に表 20-6 の対策を試してください。

表 20-6：トランスペアレントブリッジング：ループとブロードキャストストームが発生する

考えられる原因	推奨される対策
スパニングツリーが実装されていない	<ol style="list-style-type: none"> 1. インターネットワークのトポロジマップを検証し、ループの可能性を確認します。 2. 存在するループをすべて解消するか、適切なリンクがバックアップモードになっていることを確認します。 3. ブロードキャストストームとパケットループが続く場合は、show interfaces EXEC コマンドを使用して、入出力パケットカウンターの統計情報を取得します。通常のトラフィック負荷と比較して、カウンタが異常に高いレートで増加している場合は、ネットワーク内にループが残っている可能性があります。 4. スパニングツリーアルゴリズムを実装して、ループの発生を防止します。
スパニングツリーアルゴリズムのミスマッチ	<ol style="list-style-type: none"> 1. 各ブリッジで show span EXEC コマンドを使用して、どのスパニングツリーアルゴリズムが使用されているかを判別します。 2. すべてのブリッジで同一のスパニングツリーアルゴリズム (DEC または IEEE[1] のいずれか) が実装されていることを確認します。一部のきわめて特殊な構成 (一般的には IRB を含む構成) では、ネットワーク内に DEC と IEEE の両方のスパニングツリーアルゴリズムを使用することが必要となる場合があります。スパニングツリープロトコルのミスマッチを意図的に行っている場合を除き、適宜ブリッジを再設定し、すべてのブリッジで同じスパニングツリーアルゴリズムを使用するようにします。 <p>注: DEC と IEEE のスパニングツリーアルゴリズム間には互換性はありません。</p>
複数のブリッジングドメインの設定が間違っている	<ol style="list-style-type: none"> 1. ブリッジで show span EXEC コマンドを使用して、すべてのドメイングループ番号が任意のブリッジングドメインに対応することを確認します。 2. ブリッジに対して複数のドメイングループが設定されている場合は、すべてのドメインの仕様が適切に割り当てら

	<p>れていることを確認します。必要な変更を加える場合は、bridge <group> domain <domain-number> グローバル設定コマンドを使用します。</p> <p>3. ブリッジドメイン間にループが存在しないことを確認します。ドメイン間ブリッジング環境では、スパニングツリーに基づくループの防止機能は提供されていません。各ドメインのスパニングツリーは固有であり、他のドメインのスパニングツリーには依存しません。</p>
<p>リンクエラー（単方向リンク）、デュプレックスミスマッチ、ポートでの高レベルエラー</p>	<p>ブロックすべきポートがフォワーディングステートへ移行すると、ループが発生します。ポートがブロッキングステートを維持するためには、隣接するブリッジからBPDUを受信する必要があります。BPDUの消失につながるエラーは、すべてブリッジングループの原因となる可能性があります。</p> <ol style="list-style-type: none"> 1. ネットワーク図からブロッキングポートを特定します。 2. ブリッジ型ネットワークでブロックしているポートの状態を、show interface コマンドおよび show bridge EXEC コマンドを使用して確認します。 3. ブロックされている可能性があるポートが、転送中か、転送を開始しようとしていた場合（つまりラーニングあるいはリスニングステートの場合）、問題の真の原因が見つかったこととなります。そのポートがBPDUを受信しているか確認してください。受信していない場合は、おそらく、このポートに接続しているリンクに問題があります。この場合は、リンクエラー、デュプレックスの設定などを調べてください。 <p>LANポートがBPDUを受信している場合は、そのLANの代表ブリッジと考えられるブリッジを調べます。次に、ルートに向かうパス上のすべてのリンクを調べます。これらリンクの1つで問題が見つかります（最初のネットワーク図が正しいこととなります）。</p>

Cisco TAC チームへのお問い合わせの前に

お使いのネットワークが安定している場合は、そのトポロジに関する情報をできる限り収集してください。

最低でも、次のデータが必要です。

- ネットワークの物理的なトポロジ
- ルートブリッジ (およびバックアップのルートブリッジ) の予想位置
- ブロックされているポートの位置

その他の情報源

書籍 :

- 『Interconnections, Bridges and Routers, 』、ラディア・パールマン著、Addison-Wesley
- 『Cisco Lan Switching』、K.クラーク、K.ハミルトン共著、Cisco Press

関連情報

- [トランスペアレントブリッジングに関するドキュメント](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)