

# Résolution des problèmes liés aux environnements de pontage transparent

## Contenu

[Objectifs](#)

[Notions de base sur la technologie de pontage transparent](#)

[Boucles de pontage](#)

[Algorithme Spanning Tree](#)

[Format de trame](#)

[Champs de message](#)

[Différentes techniques de pontage IOS](#)

[Dépannage du pontage transparent](#)

[Pontage transparent : Aucune connectivité](#)

[Pontage transparent : Spanning Tree instable](#)

[Pontage transparent : Les sessions se terminent de manière inattendue](#)

[Pontage transparent : Des tempêtes de bouclage et de diffusion se produisent](#)

[Avant d'appeler l'équipe TAC de Cisco Systems](#)

[Sources supplémentaires](#)

[Informations connexes](#)

## Objectifs

Les ponts transparents ont été développés pour la première fois à Digital Equipment Corporation (DEC) au début des années 1980 et sont maintenant très populaires dans les réseaux Ethernet/IEEE 802.3.

- Ce chapitre définit d'abord un pont transparent comme un pont d'apprentissage qui implémente le protocole Spanning Tree. Une description détaillée du protocole Spanning Tree est incluse.
- Les périphériques Cisco qui implémentent des ponts transparents étaient auparavant répartis en deux catégories : les routeurs qui exécutent le logiciel Cisco IOS<sup>®</sup> et la gamme Catalyst de commutateurs qui exécutent des logiciels spécifiques. Ce n'est plus le cas. Plusieurs produits Catalyst sont désormais basés sur IOS. Ce chapitre présente les différentes techniques de pontage disponibles sur les périphériques IOS. Pour obtenir des informations sur la configuration et le dépannage spécifiques au logiciel Catalyst, reportez-vous au chapitre Commutation LAN.
- Enfin, nous introduisons des procédures de dépannage qui sont classées par les symptômes de problèmes potentiels qui se produisent généralement dans les réseaux de pontage transparents.

## Notions de base sur la technologie de pontage transparent

Les ponts transparents tirent leur nom du fait que leur présence et leur fonctionnement sont transparents pour les hôtes du réseau. Lorsque des ponts transparents sont mis sous tension, ils apprennent la topologie du réseau en analysant l'adresse source des trames entrantes de tous les réseaux connectés. Si, par exemple, un pont voit une trame arriver sur la ligne 1 à partir de l'hôte A, le pont conclut que l'hôte A peut être atteint via le réseau connecté à la ligne 1. Grâce à ce processus, les ponts transparents créent une table de pontage interne telle que celle du tableau 20-1.

**Tableau 20-1 : Une table de pontage transparente**

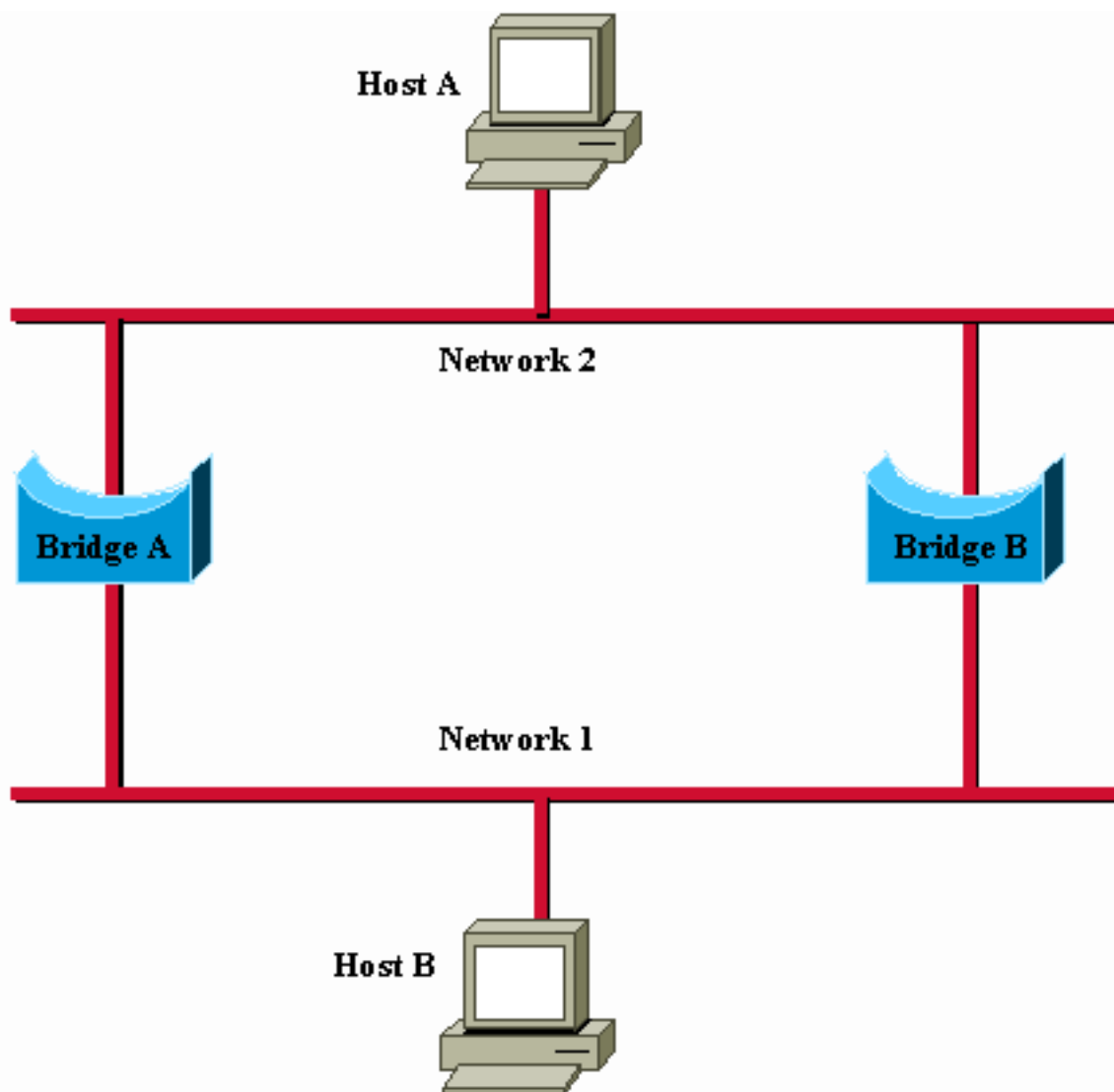
Adresse hôte	Numéro de réseau
0000.0000.0001	1
0000.b07e.ee0e	7
?	-
0050.50e1.9b80	4
0060.b0d9.2e3d	2
0000.0c8c.7088	1
?	-

Le pont utilise sa table de pontage comme base pour le transfert du trafic. Lorsqu'une trame est reçue sur l'une des interfaces de pont, le pont recherche l'adresse de destination de la trame dans sa table interne. Si la table est mappée entre l'adresse de destination et l'un des ports du pont (à l'exception de celui sur lequel la trame a été reçue), la trame est transférée au port spécifié. Si aucune carte n'est trouvée, la trame est diffusée vers tous les ports sortants. Les diffusions et les multidiffusions sont également diffusées de cette manière.

Les ponts transparents isolent correctement le trafic intra-segment et réduisent le trafic observé sur chaque segment individuel. Cela améliore généralement les temps de réponse du réseau. La mesure dans laquelle le trafic est réduit et les temps de réponse améliorés dépend du volume du trafic intersegment (par rapport au trafic total) ainsi que du volume du trafic de diffusion et de multidiffusion.

### Boucles de pontage

Sans protocole de pont à pont, l'algorithme de pont transparent échoue lorsqu'il existe plusieurs chemins de ponts et de réseaux locaux (LAN) entre deux réseaux locaux de l'interréseau. La figure 20-1 illustre une telle boucle de pontage.



**Figure 20-1 : Transfert et apprentissage inexacts dans des environnements de pontage transparents**

Supposons que l'hôte A envoie une trame à l'hôte B. Les deux ponts reçoivent la trame et concluent correctement que l'hôte A se trouve sur le réseau 2. Malheureusement, une fois que l'hôte B a reçu deux copies de la trame de l'hôte A, les deux ponts reçoivent à nouveau la trame sur leurs interfaces réseau 1, car tous les hôtes reçoivent tous les messages sur les réseaux locaux de diffusion. Dans certains cas, les ponts modifient ensuite leurs tables internes pour indiquer que l'hôte A se trouve sur le réseau 1. Si c'est le cas, lorsque l'hôte B répond à la trame de l'hôte A, les deux ponts reçoivent les réponses et les abandonnent par la suite, car leurs tables indiquent que la destination (l'hôte A) se trouve sur le même segment de réseau que la source de la trame.

Outre les problèmes de connectivité de base, tels que celui décrit, la prolifération des messages de diffusion sur les réseaux avec des boucles représente un problème réseau potentiellement grave. En référence à la figure 20-1, supposez que la trame initiale de l'hôte A est une diffusion. Les deux ponts transmettent les trames sans fin, utilisent toute la bande passante réseau disponible et bloquent la transmission d'autres paquets sur les deux segments.

Une topologie avec des boucles telles que celles illustrées à la Figure 20-1 peut être utile, ainsi que potentiellement nuisible. Une boucle implique l'existence de plusieurs chemins à travers l'interréseau. Un réseau comportant plusieurs chemins d'une source à l'autre offre ce qu'on appelle une souplesse topologique améliorée qui augmente la tolérance globale aux pannes du réseau.

## Algorithme Spanning Tree

L'algorithme Spanning Tree (STA) a été développé par DEC, un fournisseur Ethernet clé, pour préserver les avantages des boucles tout en éliminant leurs problèmes. L'algorithme DEC a ensuite été révisé par le comité IEEE 802 et publié dans la spécification IEEE 802.1d. L'algorithme DEC et l'algorithme IEEE 802.1d ne sont pas identiques, ni compatibles.

Le STA désigne un sous-ensemble sans boucle de la topologie du réseau en plaçant ces ports de pont, de sorte que, s'il est actif, il peut créer des boucles dans une condition de secours (blocage). Le blocage des ports de pont peut être activé en cas de défaillance de la liaison principale, qui fournit un nouveau chemin à travers l'interréseau.

Le STA utilise une conclusion de la théorie des graphiques comme base pour la construction d'un sous-ensemble sans boucle de la topologie du réseau. La théorie des graphiques affirme : « Pour tout graphique connecté constitué de noeuds et d'arêtes connectant des paires de noeuds, il existe un arbre recouvrant d'arêtes qui maintient la connectivité du graphique mais ne contient pas de boucles. »

La figure 20-2 illustre comment le STA élimine les boucles. Le STA appelle chaque pont à se voir attribuer un identificateur unique. En règle générale, cet identificateur est l'une des adresses MAC (Media Access Control) du pont plus une indication de priorité. Chaque port de chaque pont reçoit également un identificateur unique (au sein de ce pont) (généralement sa propre adresse MAC). Enfin, chaque port de pont est associé à un coût de chemin. Le coût du chemin représente le coût de transmission d'une trame sur un réseau local via ce port. Dans la Figure 20-2, les coûts de chemin sont indiqués sur les lignes qui proviennent de chaque pont. Les coûts de chemin sont généralement des valeurs par défaut, mais ils peuvent être attribués manuellement par les administrateurs réseau.

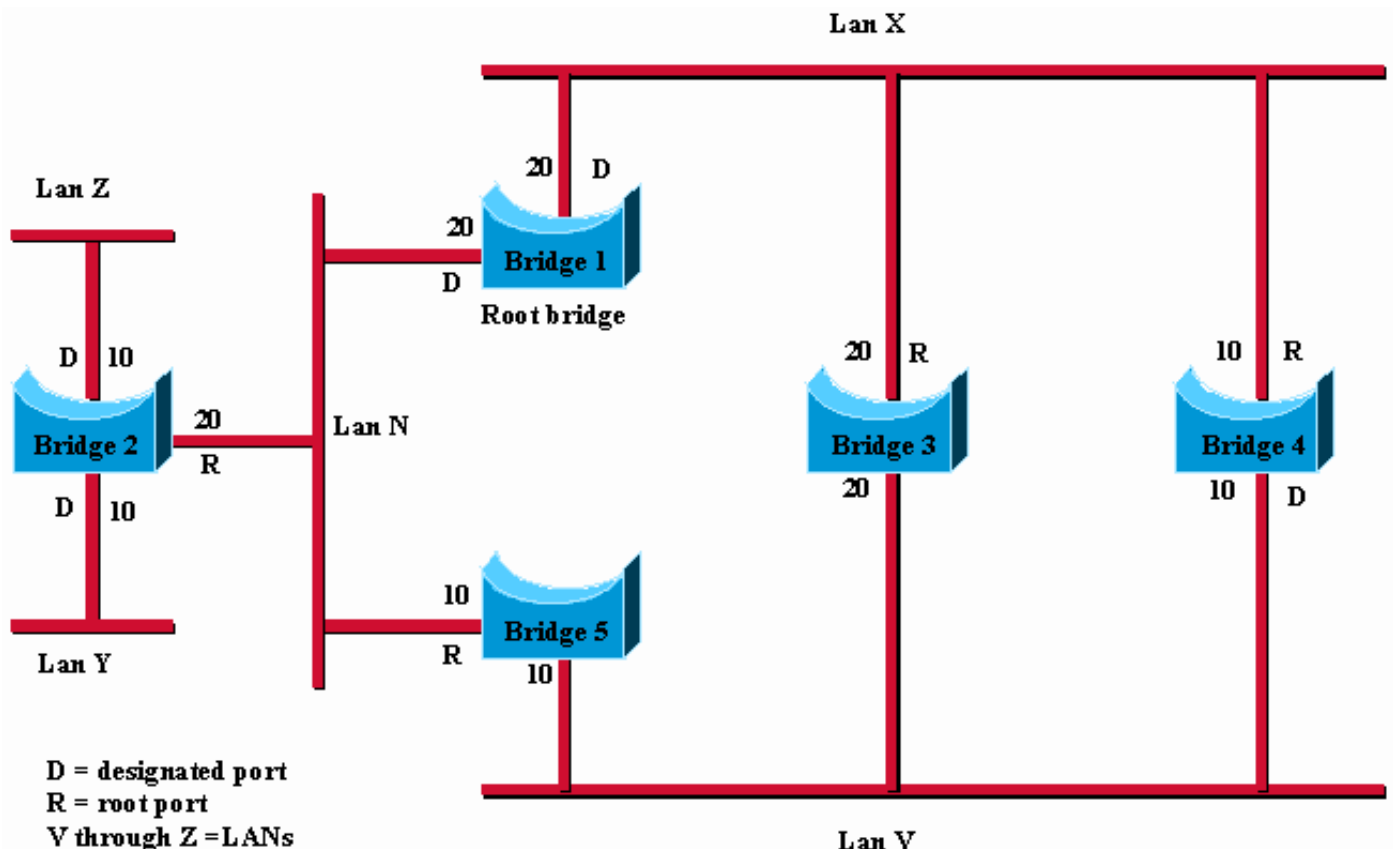


Figure 20-2 : Réseau de pont transparent (avant STA)

La première activité dans un calcul Spanning Tree est la sélection du pont racine, qui est le pont ayant la valeur d'identificateur de pont la plus faible. Dans la Figure 20-2, le pont racine est Bridge 1. Ensuite, le port racine de tous les autres ponts est déterminé. Un port racine d'un pont est le port par lequel le pont racine peut être atteint avec le coût de chemin agrégé le moins élevé. La valeur du coût de chemin agrégé le moins élevé vers la racine est appelée coût de chemin racine.

Enfin, les ponts désignés et leurs ports désignés sont déterminés. Un pont désigné est le pont sur chaque réseau local qui fournit le coût minimal du chemin racine. Un pont désigné d'un réseau local est le seul pont autorisé à transférer des trames vers et depuis le réseau local pour lequel il est le pont désigné. Un port désigné d'un réseau local est le port qui le connecte au pont désigné.

Dans certains cas, deux ponts ou plus peuvent avoir le même coût de chemin racine. Par exemple, dans la Figure 20-2, les ponts 4 et 5 peuvent atteindre le pont 1 (le pont racine) avec un coût de chemin de 10. Dans ce cas, les identificateurs de pont sont de nouveau utilisés, cette fois, pour déterminer les ponts désignés. Le port LAN V du pont 4 est sélectionné sur le port LAN V du pont 5.

Avec ce processus, tous les ponts, sauf un, directement connectés à chaque réseau local sont supprimés, ce qui supprime toutes les boucles de deux réseaux locaux. Le STA élimine également les boucles qui impliquent plus de deux LAN, tout en préservant la connectivité. La Figure 20-3 présente les résultats de l'application de l'algorithme STA au réseau, comme illustré à la Figure 20-2. La figure 20-2 illustre la topologie arborescente de manière plus claire. Une comparaison de cette figure avec la Figure 20-3 montre que le STA a placé les ports vers le LAN V dans les ponts 3 et 5 en mode veille.

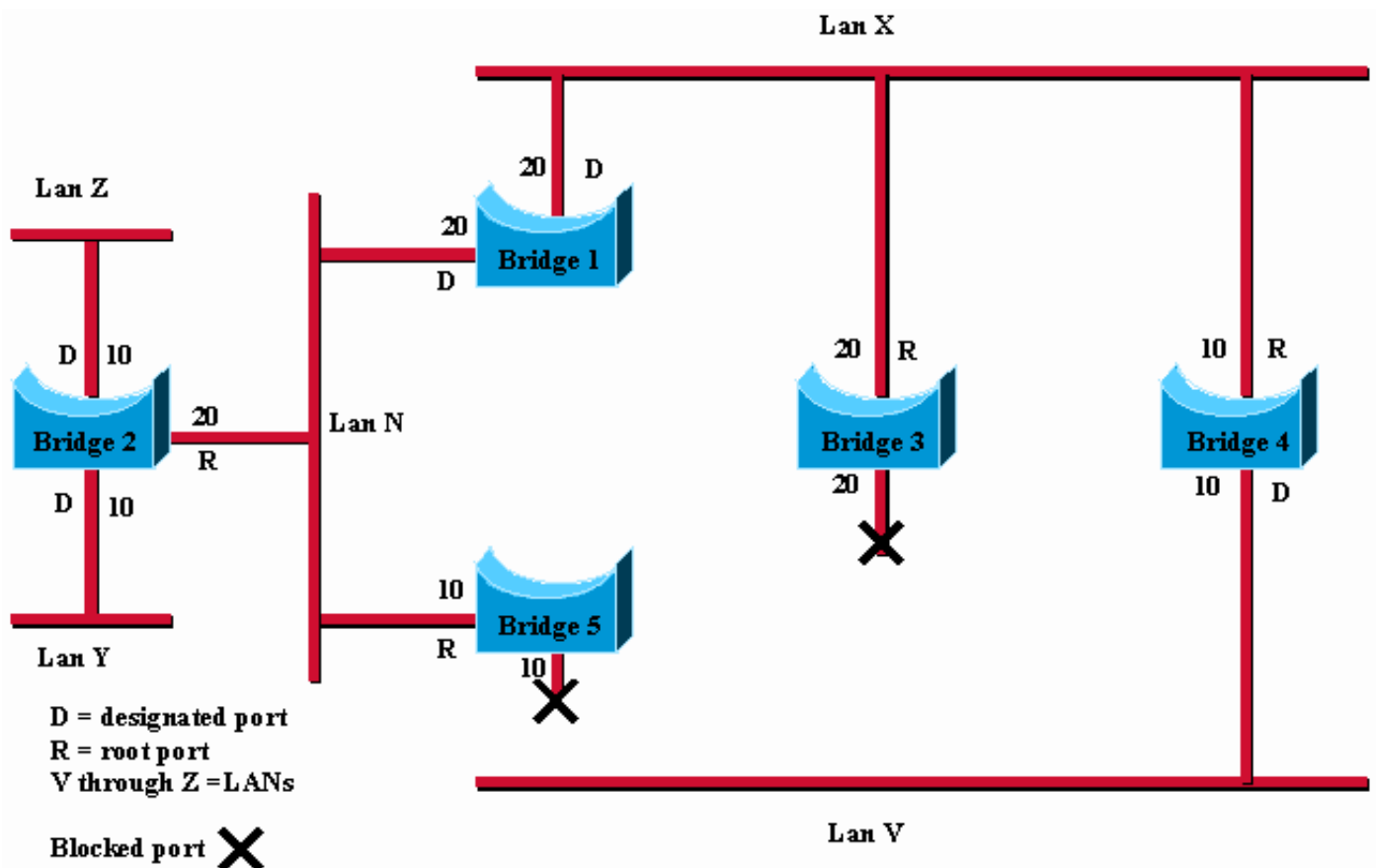


Figure 20-3 : Réseau de pont transparent (après STA)

Le calcul Spanning Tree se produit lorsque le pont est mis sous tension et lorsqu'une modification de topologie est détectée. Le calcul nécessite une communication entre les ponts Spanning Tree,

qui est effectuée par le biais de messages de configuration (parfois appelés unités de données de protocole de pont ou BPDU). Les messages de configuration contiennent des informations qui identifient le pont présumé être la racine (identificateur de racine) et la distance entre le pont émetteur et le pont racine (coût du chemin racine). Les messages de configuration contiennent également l'identificateur de pont et de port du pont émetteur et l'âge des informations contenues dans le message de configuration.

Les ponts échangent des messages de configuration à intervalles réguliers (généralement une à quatre secondes). Si un pont tombe en panne (ce qui entraîne une modification de la topologie), les ponts voisins détectent rapidement le manque de messages de configuration et lancent un recalcul du Spanning Tree.

Toutes les décisions relatives à la topologie des ponts sont prises localement. Les messages de configuration sont échangés entre les ponts voisins. Il n'existe aucune autorité centrale sur la topologie ou l'administration du réseau.

## Format de trame

Les ponts transparents échangent des messages de configuration et des messages de modification de topologie. Des messages de configuration sont envoyés entre les ponts pour établir une topologie de réseau. Les messages de modification de topologie sont envoyés après qu'une modification de topologie a été détectée pour indiquer que le STA doit être réexécuté.

Le tableau 20-2 présente le format du message de configuration IEEE 802.1d.

**Tableau 20-2 : Configuration transparente du pont**

Identificateur de protocole	Version	Type de message :	Indicateurs	ID de racine	Coût de chemin racine	ID de pont	ID du port	Âge du message	Âge maximal	Délai Hello	Délai de transmission
2 bytes	1 octet	1 octet	1 octet	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes

## Champs de message

Les messages de configuration de pont transparent se composent de 35 octets. Voici les champs de message :

- Identificateur de protocole: Contient la valeur 0.
- Version : Contient la valeur 0.
- Message Type : Contient la valeur 0.

- Indicateur : Champ d'un octet, dont seuls les deux premiers bits sont utilisés. Le bit de modification de topologie (TC) signale un changement de topologie. Le bit d'accusé de réception de modification de topologie (TCA) est configuré pour accuser réception d'un message de configuration avec le bit TC défini.
- ID de racine: Identifie le pont racine et répertorie sa priorité de 2 octets suivie de son ID de 6 octets.
- Coût de chemin racine: Contient le coût du chemin à partir du pont qui envoie le message de configuration au pont racine.
- ID de pont: Identifie la priorité et l'ID du pont qui envoie le message.
- ID du port: Identifie le port à partir duquel le message de configuration a été envoyé. Ce champ permet de détecter et de traiter les boucles créées par plusieurs ponts reliés.
- Âge du message: Spécifie le temps écoulé depuis que la racine a envoyé le message de configuration sur lequel le message de configuration actuel est basé.
- Âge maximum : Indique quand le message de configuration actuel doit être supprimé.
- Délai Hello: Fournit la période entre les messages de configuration du pont racine.
- Délai de transmission: Indique le temps que les ponts doivent attendre avant de passer à un nouvel état après une modification de topologie. Si un pont passe trop tôt, toutes les liaisons réseau ne peuvent pas être prêtes à changer d'état et des boucles peuvent en résulter.

Le format du message de modification de la topologie est similaire à celui du message de configuration de pont transparent, sauf qu'il se compose uniquement des quatre premiers octets. Voici les champs de message :

- Identificateur de protocole: Contient la valeur 0.
- Version : Contient la valeur 0.
- Message Type : Contient la valeur 128.

## Différentes techniques de pontage IOS

Les routeurs Cisco proposent trois méthodes différentes pour implémenter le pontage : Comportement par défaut, Routage et pontage simultanés (CRB) et Routage et pontage intégrés (IRB).

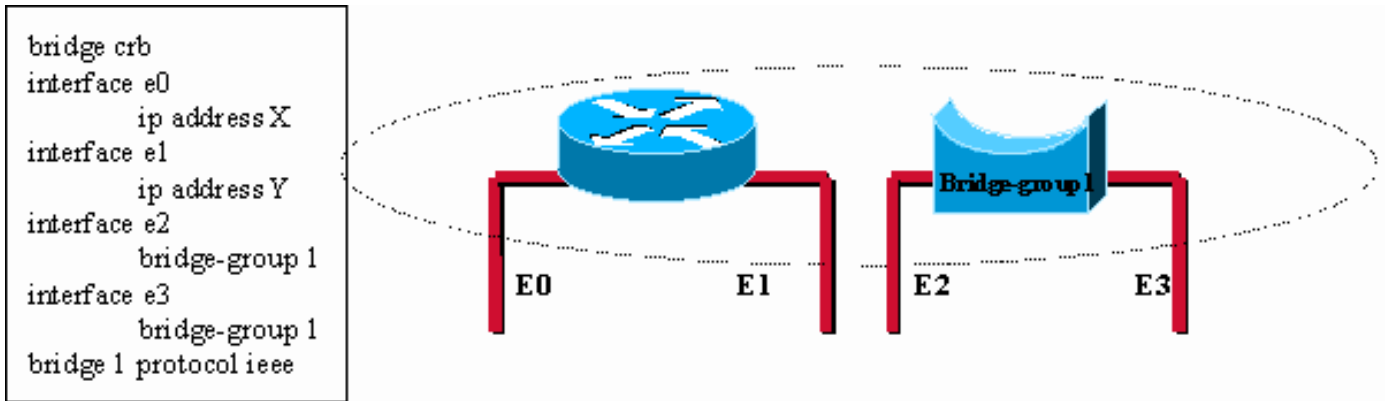
### Comportement par défaut

Avant que les fonctionnalités IRB et CRB ne soient disponibles, vous n'étiez en mesure de relier ou de router un protocole que sur une plate-forme. En d'autres termes, si la commande **ip route** était utilisée, par exemple, le routage IP était effectué sur toutes les interfaces. Dans ce cas, IP n'a pu être ponté sur aucune des interfaces du routeur.

### Routage et pontage simultanés (CRB)

Avec CRB, vous pouvez déterminer s'il faut établir un pont ou acheminer un protocole sur une base d'interface. Autrement dit, vous pouvez router un protocole donné sur certaines interfaces et relier le même protocole sur des interfaces de groupe de ponts au sein du même routeur. Le routeur peut alors être à la fois un routeur et un pont pour un protocole donné, mais il ne peut y avoir aucun type de communication entre les interfaces définies par routage et les interfaces de groupe de ponts.

Cet exemple montre que, pour un protocole donné, un seul routeur peut logiquement agir en tant que périphériques indépendants séparés : un routeur et un ou plusieurs ponts :



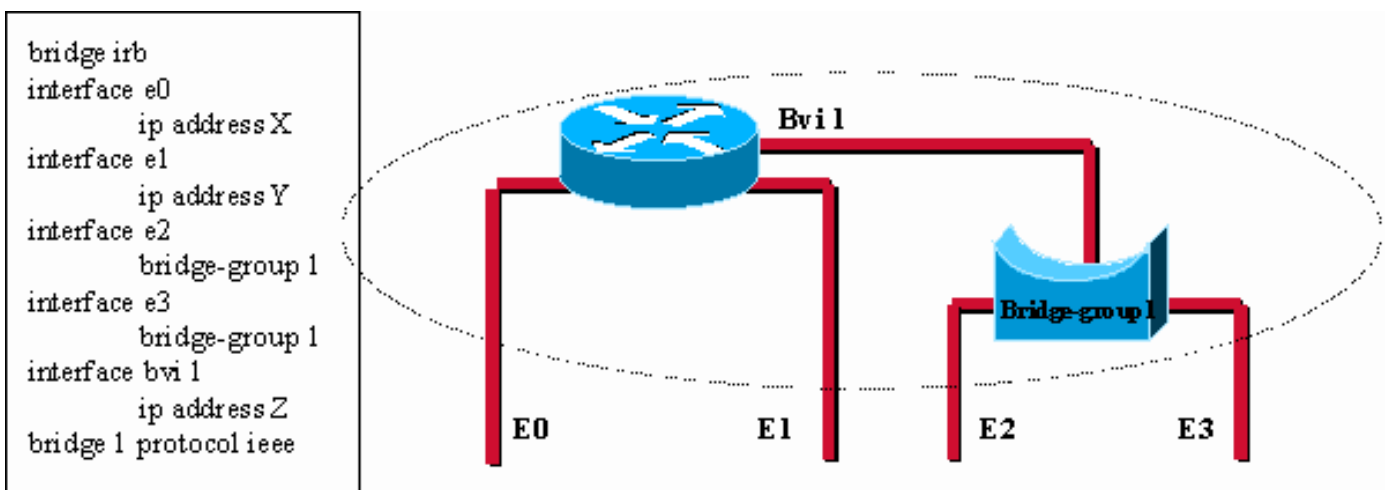
In this configuration, for the IP protocol, the Cisco device is acting like a router for interface e0 and e1 and is acting like a bridge for interface e2 and e3. Note that there is no communication possible between the two functions (a host connected on e0 would never be able to reach a host connected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

Figure 20-4 : Routage et pontage simultanés (CRB)

### Integrated Routing and Bridging (IRB)

IRB permet de router entre un groupe de ponts et une interface routée avec un concept appelé interface virtuelle de groupe de ponts (BVI). Comme le pontage se produit au niveau de la couche liaison de données et le routage au niveau de la couche réseau, ils ont différents modèles de configuration de protocole. Avec IP, par exemple, les interfaces de groupe de ponts appartiennent au même réseau et ont une adresse réseau IP collective, tandis que chaque interface routée représente un réseau distinct avec sa propre adresse réseau IP.

Le concept de BVI a été créé pour permettre à ces interfaces d'échanger des paquets pour un protocole donné. Sur le plan conceptuel, comme illustré dans cet exemple, le routeur Cisco ressemble à un routeur connecté à un ou plusieurs groupes de ponts :



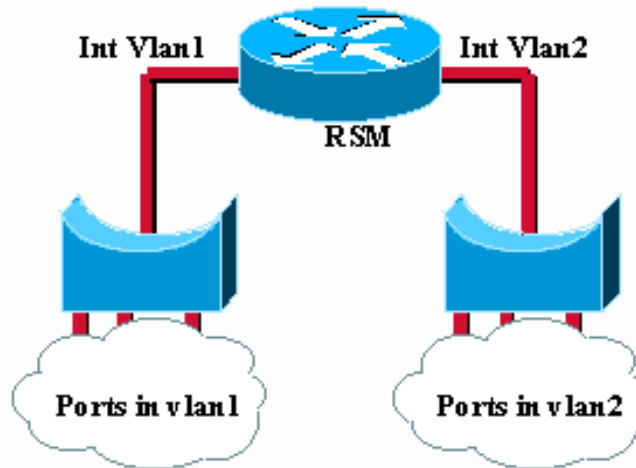
The bridge group virtual interface brings routing to bridge-group 1. One can assign an Ip address to the whole bridge-group and routed communication is now possible between a host connected to E0 and a host connected to E2 for instance.

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



L'interface BVI est une interface virtuelle au sein du routeur qui agit comme une interface routée normale. Le BVI représente le groupe de pontage correspondant aux interfaces routées au sein du routeur. Le numéro d'interface BVI est le numéro du groupe de ponts représenté par cette interface virtuelle. Le numéro est le lien entre cette BVI et le groupe de ponts.

Cet exemple montre comment le principe BVI s'applique au module de commutation de route (RSM) dans un commutateur Catalyst :



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).

Figure 20-6 : Router Switch Module (RSM) dans un commutateur Catalyst.

## Dépannage du pontage transparent

Cette section présente des informations de dépannage pour les problèmes de connectivité dans les interréseaux de pontage transparents. Il décrit les symptômes spécifiques de pontage transparent, les problèmes susceptibles de provoquer chaque symptôme et les solutions à ces problèmes.

**Remarque :** Les problèmes associés au pontage SRB (Source-Route Bridging), au pontage de traduction et au pontage SRT (Source-Route transparent) sont traités dans le chapitre 10, « Dépannage d'IBM ».

Pour dépanner efficacement votre réseau ponté, vous devez avoir une connaissance de base de sa conception, en particulier lorsqu'un Spanning Tree est impliqué.

Celles-ci doivent être disponibles :

- Carte topologique du réseau ponté
- Emplacement du pont racine
- Emplacement de la liaison redondante (et des ports bloqués)

Lorsque vous dépannez des problèmes de connectivité, réduisez le problème à un nombre minimal d'hôtes, idéalement seulement un client et un serveur.

Ces sections décrivent les problèmes réseau les plus courants dans les réseaux pontés transparents :

- [Pontage transparent : Aucune connectivité](#)
- [Pontage transparent : Spanning Tree instable](#)
- [Pontage transparent : Les sessions se terminent de manière inattendue](#)
- [Pontage transparent : Des tempêtes de bouclage et de diffusion se produisent](#)

## Pontage transparent : Aucune connectivité

**Symptôme** : Le client ne peut pas se connecter aux hôtes sur un réseau ponté de manière transparente.

Le tableau 20-3 présente les problèmes qui peuvent causer ce symptôme et propose des solutions.

**Tableau 20-3 : Pontage transparent : Aucune connectivité**

Causés possibles	Actions suggérées
Problème matériel ou média	<ol style="list-style-type: none"> <li>1. Utilisez la commande EXEC <b>show bridge</b> pour voir s'il y a un problème de connectivité. Si c'est le cas, le résultat n'affiche aucune adresse MAC[1] dans la table de pontage.</li> <li>2. Utilisez la commande EXEC <b>show interfaces</b> pour déterminer si l'interface et le protocole de ligne sont actifs.</li> <li>3. Si l'interface est en panne, dépannez le matériel ou le support. Reportez-vous au chapitre 3, « Dépannage des problèmes matériels et de démarrage ».</li> <li>4. Si le protocole de ligne est désactivé, vérifiez la connexion physique entre l'interface et le réseau. Assurez-vous que la connexion est sécurisée et que les câbles ne sont pas endommagés.</li> </ol> <p>Si le protocole de ligne est actif mais que les compteurs de paquets d'entrée et de sortie ne sont pas incrémentés, vérifiez la connectivité du support et de l'hôte. Reportez-vous au chapitre de dépannage des supports qui couvre le type de support utilisé dans votre réseau.</p>
Hôte arrêté	<ol style="list-style-type: none"> <li>1. Utilisez la commande EXEC <b>show bridge</b> sur les ponts pour vous assurer que la table de pontage inclut les adresses MAC des noeuds finaux connectés. La table de pontage comprend les adresses MAC source et de destination des hôtes et est remplie lorsque des paquets provenant d'une source ou d'une destination traversent le pont.</li> </ol>

	<ol style="list-style-type: none"> <li>2. Si des noeuds finaux attendus sont manquants, vérifiez l'état des noeuds pour vérifier qu'ils sont connectés et correctement configurés.</li> <li>3. Réinitialisez ou reconfigurez les noeuds d'extrémité si nécessaire et réexaminez la table de pontage à l'aide de la commande <b>show bridge</b>.</li> </ol>
<p>Le chemin de pontage est rompu</p>	<ol style="list-style-type: none"> <li>1. Identifier le chemin que les paquets doivent emprunter entre les noeuds d'extrémité. S'il y a un routeur sur ce chemin, divisez le dépannage en deux parties : Noeud 1-Router et Router-Node 2.</li> <li>2. Connectez-vous à chaque pont sur le chemin et vérifiez l'état des ports utilisés sur le chemin entre les noeuds d'extrémité (comme décrit dans l'entrée du tableau « Problème matériel ou média »).</li> <li>3. Utilisez la commande <b>show bridge</b> pour vous assurer que l'adresse MAC des noeuds est apprise sur les ports appropriés. Si ce n'est pas le cas, la topologie Spanning Tree peut être instable. Voir le tableau 20-2, « Pontage transparent : Spanning Tree instable. »</li> <li>4. Vérifiez l'état des ports à l'aide de la commande <b>show span</b>. Si les ports qui peuvent transmettre le trafic entre les noeuds d'extrémité ne sont pas en état de transmission, la topologie de votre arborescence peut avoir changé de manière inattendue. Voir Tableau 20-4, « Transparent Bridging Unstable Spanning Tree. »</li> </ol>
<p>Filtres de pontage mal configurés</p>	<ol style="list-style-type: none"> <li>1. Utilisez la commande d'exécution privilégiée <b>show running-config</b> pour déterminer si les filtres de pont sont configurés.</li> <li>2. Désactivez les filtres de pont sur les interfaces suspectes et déterminez si la connectivité est restaurée.</li> <li>3. Si la connectivité n'est pas restaurée, le filtre n'est pas le problème. Si la connectivité est restaurée après la suppression des filtres, un ou plusieurs filtres défectueux sont la cause du problème de connectivité.</li> <li>4. Si plusieurs filtres existent ou s'il existe des filtres qui utilisent des listes d'accès avec plusieurs instructions, appliquez chaque filtre individuellement pour identifier le filtre de</li> </ol>

	<p>problème. Vérifiez la configuration pour l'entrée et la sortie <b>LSAP</b>[2] et les filtres <b>TYPE</b>, qui peuvent être utilisés simultanément pour bloquer différents protocoles. Par exemple, <b>LSAP (F0F0)</b> peut être utilisé pour bloquer NetBIOS et <b>TYPE (6004)</b> peut être utilisé pour bloquer le transport local.</p> <p>5. Modifiez les filtres ou les listes d'accès qui bloquent le trafic. Continuez à tester les filtres jusqu'à ce que tous les filtres soient activés et que les connexions fonctionnent toujours.</p>
Files d'attente d'entrée et de sortie pleines	<p>Un trafic de multidiffusion ou de diffusion excessif peut entraîner un débordement des files d'attente d'entrée et de sortie, ce qui entraîne l'abandon des paquets.</p> <ol style="list-style-type: none"> <li>1. Utilisez la commande <b>show interfaces</b> pour rechercher les pertes d'entrée et de sortie. Les abandons suggèrent un trafic excessif sur les supports. Si le nombre actuel de paquets sur la file d'attente d'entrée est constamment égal ou supérieur à 80 % de la taille actuelle de la file d'attente d'entrée, la taille de la file d'attente d'entrée doit être ajustée pour tenir compte du débit de paquets. Même si le nombre actuel de paquets sur la file d'attente d'entrée ne semble jamais approcher la taille de la file d'attente d'entrée, les rafales de paquets peuvent toujours déborder de la file d'attente.</li> <li>2. Réduisez le trafic de diffusion et de multidiffusion sur les réseaux connectés en utilisant des filtres de pontage ou segmentez le réseau avec plus de périphériques interréseau.</li> <li>3. Si la connexion est une liaison série, augmentez la bande passante, appliquez des files d'attente prioritaires, augmentez la taille de la file d'attente de mise en attente ou modifiez la taille de la mémoire tampon système. Pour plus d'informations, reportez-vous au Chapitre 15, « Dépannage des problèmes de ligne série ».</li> </ol>

[1]MAC = Contrôle d'accès au support

[2]LSAP = Point d'accès aux services de liaison

## Pontage transparent : Spanning Tree instable

**Symptôme** : Perte transitoire de la connectivité entre les hôtes. Plusieurs hôtes sont affectés en même temps.

Le tableau 20-4 présente les problèmes qui peuvent causer ce symptôme et propose des solutions.

Tableau 20-4 : Pontage transparent : Spanning Tree instable

Caus es possi bles	Actions suggérées
Lien clign otant	<ol style="list-style-type: none"><li>1. Utilisez la commande <b>show span</b> pour voir si le nombre de modifications de topologie augmente régulièrement.</li><li>2. Si oui, vérifiez la liaison entre vos ponts à l'aide de la commande <b>show interface</b>. Si cette commande ne révèle pas de liaison qui clignote entre deux ponts, utilisez la commande EXEC privilégiée <b>debug spantree event</b> sur vos ponts.</li></ol> <p>Cette option enregistre toutes les modifications liées au Spanning Tree. Dans une topologie stable, il ne peut y en avoir aucune. Les seules liaisons à suivre sont celles qui relient les périphériques du pont. Une transition sur une liaison à une station d'extrémité ne doit avoir aucun impact sur le réseau.</p> <p><b>Remarque</b> : Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus CPU, l'utilisation de la commande <b>debug spantree event</b> peut rendre le système inutilisable. Pour cette raison, utilisez les commandes <b>debug</b> uniquement pour résoudre des problèmes spécifiques ou lors de sessions pour résoudre des problèmes avec le personnel d'assistance technique de Cisco. En outre, il est préférable d'utiliser les commandes <b>debug</b> dans les périodes de faible trafic réseau et de moins d'utilisateurs. Si vous effectuez un débogage au cours de ces périodes, cela diminue la probabilité que l'augmentation des processus de surcharge de <b>débogage</b> affecte l'utilisation du système.</p>
Le pont racin e conti nue	<ol style="list-style-type: none"><li>1. Vérifiez la cohérence des informations de pont racine sur l'ensemble du réseau ponté avec les commandes <b>show span</b> sur les différents ponts.</li><li>2. Si plusieurs ponts prétendent être la racine,</li></ol>

de changer/ plusieurs ponts prétendent être la racine	<p>assurez-vous d'exécuter le même protocole Spanning Tree sur chaque pont (voir l'entrée de table de l'algorithme Spanning Tree non-correspondance dans le tableau 20-6).</p> <ol style="list-style-type: none"> <li>Utilisez la commande <b>bridge &lt;group&gt; priority &lt;number&gt;</b> sur le pont racine pour forcer le pont souhaité à devenir la racine. Plus la priorité est faible, plus il est probable que le pont devienne la racine.</li> <li>Vérifiez le diamètre de votre réseau. Avec un Spanning Tree standard configuré, il ne doit jamais y avoir plus de sept sauts de pont entre deux hôtes.</li> </ol>
Hello s non échangés	<ol style="list-style-type: none"> <li>Vérifiez si les ponts communiquent entre eux. Utilisez un analyseur de réseau ou la commande d'exécution privilégiée <b>debug spantree tree</b> pour voir si les trames Hello spanning tree sont échangées. <b>Remarque :</b> Étant donné que la sortie de débogage se voit attribuer une priorité élevée dans le processus CPU, l'utilisation de la commande <b>debug spantree event</b> peut rendre le système inutilisable. Pour cette raison, utilisez les commandes <b>debug</b> uniquement pour résoudre des problèmes spécifiques ou lors de sessions pour résoudre des problèmes avec le personnel d'assistance technique de Cisco. En outre, il est préférable d'utiliser les commandes <b>debug</b> dans les périodes de faible trafic réseau et de moins d'utilisateurs. Si vous effectuez un débogage au cours de ces périodes, cela diminue la probabilité que l'augmentation des processus de surcharge de <b>débogage</b> affecte l'utilisation du système.</li> <li>Si aucun hellos n'est échangé, vérifiez les connexions physiques et la configuration logicielle sur les ponts.</li> </ol>

## [Pontage transparent : Les sessions se terminent de manière inattendue](#)

**Symptôme :** Les connexions dans un environnement ponté de manière transparente sont établies avec succès, mais les sessions se terminent parfois brusquement.

Le tableau 20-5 présente les problèmes qui peuvent causer ce symptôme et propose des solutions.

**Tableau 20-5 : Pontage transparent : Les sessions se terminent de manière inattendue**

Causes possibles	Actions suggérées
Retransmissions excessives	<ol style="list-style-type: none"> <li>1. Utilisez un analyseur de réseau pour rechercher les retransmissions d'hôtes.</li> <li>2. Si vous voyez des retransmissions sur des lignes série lentes, augmentez les minuteurs de transmission sur l'hôte. Pour plus d'informations sur la configuration de vos hôtes, reportez-vous à la documentation du fournisseur. Pour plus d'informations sur le dépannage des lignes série, reportez-vous au Chapitre 15, « Dépannage des problèmes de ligne série ». Si vous voyez des retransmissions sur un support LAN à haut débit, vérifiez si les paquets sont envoyés et reçus dans l'ordre ou abandonnés par tout périphérique intermédiaire (tel qu'un pont ou un commutateur). Dépannez le support LAN, le cas échéant. Pour plus d'informations, reportez-vous au chapitre sur le dépannage des supports qui couvrent le type de support utilisé dans votre réseau.</li> <li>3. Utilisez un analyseur de réseau pour déterminer si le nombre de retransmissions diminue.</li> </ol>
Délai excessif sur la liaison série	Augmentez la bande passante, appliquez la file d'attente prioritaire, augmentez la taille de la file d'attente de mise en attente ou modifiez la taille de la mémoire tampon système. Pour plus d'informations, reportez-vous au Chapitre 15, « Dépannage des problèmes de ligne série ».

## Pontage transparent : Des tempêtes de bouclage et de diffusion se produisent

**Symptôme** : Les boucles de paquets et les tempêtes de diffusion se produisent dans des environnements de ponts transparents. Les stations d'extrémité sont contraintes à une retransmission excessive, ce qui entraîne l'expiration ou l'abandon des sessions.

**Remarque** : Les boucles de paquets sont généralement causées par des problèmes de conception de réseau ou de matériel.

Le tableau 20-6 présente les problèmes qui peuvent causer ce symptôme et propose des solutions.

Les boucles de pontage sont le scénario le plus défavorable dans un réseau ponté, car elles peuvent avoir un impact sur chaque utilisateur. En cas d'urgence, la meilleure façon de récupérer

rapidement la connectivité est de désactiver manuellement toutes les interfaces qui fournissent un chemin redondant dans le réseau. Malheureusement, la cause de la boucle de pontage sera très difficile à identifier par la suite si vous le faites. Si possible, essayez d'effectuer les actions du tableau 20-6 au préalable.

**Tableau 20-6 : Pontage transparent : Des tempêtes de bouclage et de diffusion se produisent**

Causes possibles	Actions suggérées
Aucun Spanning Tree implémenté	<ol style="list-style-type: none"> <li>1. Examinez une carte topologique de votre interréseau pour vérifier s'il existe des boucles possibles.</li> <li>2. Éliminez les boucles existantes ou assurez-vous que les liaisons appropriées sont en mode de sauvegarde.</li> <li>3. Si les tempêtes de diffusion et les boucles de paquets persistent, utilisez la commande EXEC <b>show interfaces</b> pour obtenir des statistiques de nombre de paquets d'entrée et de sortie. Si ces compteurs s'incrémentent à un débit anormalement élevé (par rapport à vos charges de trafic normales), une boucle est probablement toujours présente dans le réseau.</li> <li>4. Implémentez un algorithme Spanning Tree pour empêcher les boucles.</li> </ol>
Incompatibilité de l'algorithme Spanning Tree	<ol style="list-style-type: none"> <li>1. Utilisez la commande EXEC <b>show span</b> sur chaque pont pour déterminer quel algorithme Spanning Tree est utilisé.</li> <li>2. Assurez-vous que tous les ponts exécutent le même algorithme Spanning Tree (DEC ou IEEE)[1]. Il peut être nécessaire d'utiliser les algorithmes Spanning Tree DEC et IEEE dans le réseau pour certaines configurations très spécifiques (généralement, celles qui impliquent IRB). Si la non-correspondance dans le protocole Spanning Tree n'est pas prévue, reconfigurez les ponts de manière à ce que tous les ponts utilisent le même algorithme Spanning Tree.</li> </ol> <p><b>Remarque :</b> Les algorithmes Spanning Tree DEC et IEEE sont incompatibles.</p>
Plusieurs domaines	<ol style="list-style-type: none"> <li>1. Utilisez la commande EXEC <b>show span</b> sur les ponts pour vous assurer que tous</li> </ol>



<p>de pontage mal configurés</p>	<p>les numéros de groupe de domaines correspondent à des domaines de pontage donnés.</p> <ol style="list-style-type: none"> <li>2. Si plusieurs groupes de domaines sont configurés pour le pont, assurez-vous que toutes les spécifications de domaine sont attribuées correctement. Utilisez la commande de configuration globale <b>bridge &lt;group&gt; domain &lt;domain-number&gt;</b> pour apporter les modifications nécessaires.</li> <li>3. Assurez-vous qu'il n'existe aucune boucle entre les domaines de pontage. Un environnement de pontage interdomaine ne fournit pas de prévention des boucles basée sur le protocole Spanning Tree. Chaque domaine a son propre Spanning Tree, qui est indépendant du Spanning Tree dans d'autres domaines.</li> </ol>
<p>Erreur de liaison (liaison unidirectionnelle), incompatibilité de mode duplex, niveau élevé d'erreur sur un port.</p>	<p>Les boucles se produisent lorsqu'un port qui doit bloquer passe à l'état de transmission. Un port doit recevoir des BPDU d'un pont voisin afin de rester à l'état de blocage. Toute erreur conduisant à des BPDU perdus peut alors être la cause d'une boucle de pontage.</p> <ol style="list-style-type: none"> <li>1. Identifiez les ports de blocage de votre schéma de réseau.</li> <li>2. Vérifiez l'état des ports qui doivent bloquer dans votre réseau ponté à l'aide des commandes EXEC <b>show interface</b> et <b>show bridge</b>.</li> <li>3. Si vous trouvez un port potentiellement bloqué qui est en cours de transfert ou sur le point de le transférer (c'est-à-dire, dans l'état d'apprentissage ou d'écoute), vous avez trouvé la véritable source du problème. Vérifiez si ce port reçoit des BPDU. Si ce n'est pas le cas, il y a probablement un problème sur la liaison connectée à ce port. Vérifiez ensuite les erreurs de liaison, les paramètres de duplex, etc.).</li> </ol> <p>Si le port reçoit toujours des BPDU, accédez au pont que vous prévoyez d'attribuer à ce réseau local. Vérifiez ensuite tous les liens du chemin vers la racine. Vous trouverez un problème sur l'une de ces liaisons (à condition que votre schéma de réseau initial soit</p>

correct).
-----------

[1]IEEE = Institut des ingénieurs électriques et électroniques

## [Avant d'appeler l'équipe TAC de Cisco Systems](#)

Lorsque votre réseau est stable, collectez autant d'informations que possible sur sa topologie.

Collectez au minimum ces données :

- Topologie physique du réseau
- Emplacement prévu du pont racine (et du pont racine de secours)
- Emplacement des ports bloqués

## [Sources supplémentaires](#)

Livres :

- Interconnexions, ponts et routeurs, Radia Perlman, Addison-Wesley
- Commutation Lan Cisco, K.Clark, K.Hamilton, Cisco Press

## [Informations connexes](#)

- [Documentation de pontage transparent](#)
- [Support et documentation techniques - Cisco Systems](#)