Fehlerbehebung in transparenten Bridging-Umgebungen

Inhalt

Ziele

Transparente Brücken wurden Anfang der 1980er Jahre bei der Digital Equipment Corporation (DEC) entwickelt und sind heute in Ethernet/IEEE 802.3-Netzwerken sehr beliebt.

- In diesem Kapitel wird zunächst eine transparente Bridge als Learning Bridge definiert, die das Spanning Tree-Protokoll implementiert. Eine ausführliche Beschreibung des Spanning Tree-Protokolls ist enthalten.
- Cisco Geräte, die transparente Bridges implementieren, wurden in zwei Kategorien unterteilt: Router, auf denen die Cisco IOS® Software und die Catalyst-Switches ausgeführt werden, auf denen spezifische Software ausgeführt wird. Das ist nicht mehr der Fall. Einige Catalyst-Produkte basieren jetzt auf IOS. In diesem Kapitel werden die verschiedenen Bridging-Techniken vorgestellt, die auf IOS-Geräten verfügbar sind. Informationen zur softwarespezifischen Konfiguration und Fehlerbehebung von Catalyst finden Sie im Kapitel LAN-Switching.
- Schließlich führen wir einige Fehlerbehebungsverfahren ein, die anhand der Symptome potenzieller Probleme klassifiziert werden, die typischerweise in transparenten Bridging-Netzwerken auftreten.

Grundlagen der transparenten Bridging-Technologie

Transparente Bridges leiten ihren Namen davon ab, dass ihre Präsenz und ihr Betrieb für Netzwerkhosts transparent sind. Wenn transparente Bridges eingeschaltet werden, lernen sie die Topologie des Netzwerks durch Analyse der Quelladresse eingehender Frames aus allen angeschlossenen Netzwerken. Wenn beispielsweise eine Bridge einen Frame von Host A auf Leitung 1 ankommt, kommt die Bridge zu dem Schluss, dass Host A über das mit Leitung 1 verbundene Netzwerk erreicht werden kann. Durch diesen Prozess erstellen transparente Bridges eine interne Bridging-Tabelle wie die in Tabelle 20-1.

Tabelle 20-1: Transparente Bridging-Tabelle

Hostadresse	Netzwerknummer
0000.0000.0001	1
0000.b07e.ee0e	7
?	-
0050,50e1,9b80	4
0060.b0d9.2e3d	2
0000,0c8c,7088	1
?	-

Die Bridge verwendet ihre Bridging-Tabelle als Grundlage für die Weiterleitung des Datenverkehrs. Wenn ein Frame auf einer der Bridge-Schnittstellen empfangen wird, sucht die Bridge die Zieladresse des Frames in der internen Tabelle. Wenn die Tabelle zwischen der Zieladresse und einem der Ports der Bridge (außer dem Port, an dem der Frame empfangen wurde) zugeordnet ist, wird der Frame an den angegebenen Port weitergeleitet. Wenn keine Zuordnung gefunden wird, wird der Frame an alle ausgehenden Ports überflutet. Broadcasts und Multicasts werden ebenfalls auf diese Weise überflutet.

Transparente Bridges können den Datenverkehr innerhalb von Segmenten erfolgreich isolieren und den Datenverkehr in jedem einzelnen Segment reduzieren. Dadurch werden in der Regel die Reaktionszeiten im Netzwerk verbessert. Das Ausmaß, in dem der Datenverkehr reduziert und die Reaktionszeiten verbessert werden, hängt vom Datenverkehr zwischen Segmenten (bezogen auf den Gesamtverkehr) sowie vom Broadcast- und Multicast-Datenverkehr ab.

Bridging-Loops

Ohne ein Bridge-to-Bridge-Protokoll schlägt der transparente Bridge-Algorithmus fehl, wenn mehrere Bridges und LANs (Local Area Networks) zwischen zwei beliebigen LANs im Internet vorhanden sind. Abbildung 20-1 zeigt eine solche Bridging-Schleife.

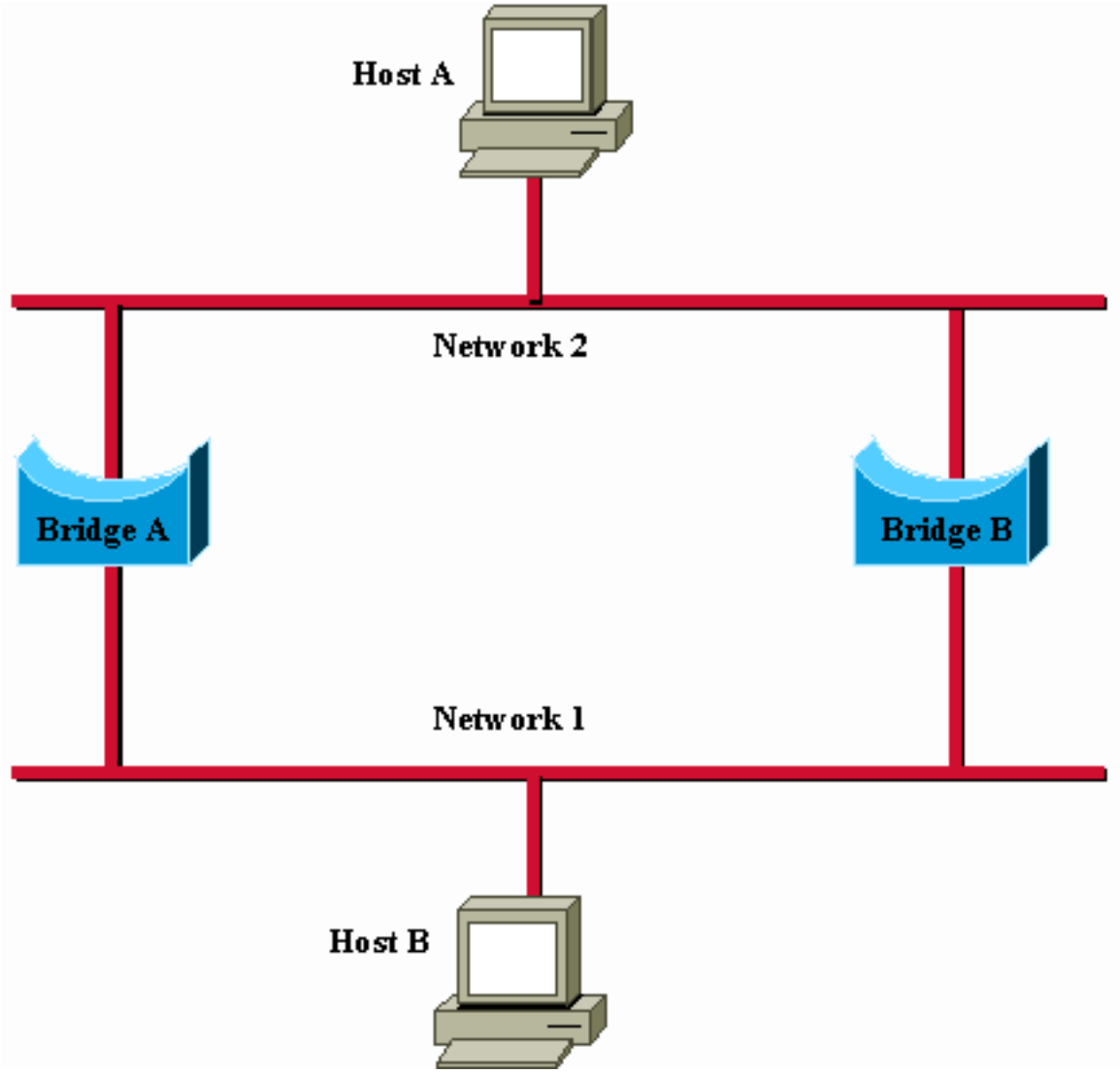


Abbildung 20-1: Ungenaue Weiterleitung und Schulung in transparenten Bridging-Umgebungen

Beispiel: Host A sendet einen Frame an Host B. Beide Brücken empfangen den Frame und schließen korrekt, dass Host A auf Netzwerk 2 ist. Nachdem Host B zwei Kopien des Frames von Host A empfängt, erhalten beide Bridges leider erneut den Frame auf ihren Netzwerk 1-Schnittstellen, da alle Hosts alle Nachrichten in Broadcast-LANs empfangen. In einigen Fällen ändern die Bridges dann ihre internen Tabellen, um anzuzeigen, dass Host A auf Netzwerk 1 ist. Wenn dies der Fall ist, erhalten und verwerfen beide Brücken, wenn Host B auf den Frame von Host A antwortet, Antworten, da ihre Tabellen darauf hinweisen, dass sich das Ziel (Host A) im gleichen Netzwerksegment befindet wie die Quelle des Frames.

Neben grundlegenden Verbindungsproblemen wie dem beschriebenen stellt die Verbreitung von Broadcast-Nachrichten in Netzwerken mit Schleifen ein potenziell schwerwiegendes Netzwerkproblem dar. Gehen Sie in Bezug auf Abbildung 20-1 davon aus, dass der ursprüngliche Frame von Host A eine Broadcast-Übertragung ist. Beide Brücken leiten die Frames endlos weiter, nutzen die gesamte verfügbare Netzwerkbandbreite und blockieren die Übertragung anderer Pakete in beiden Segmenten.

Eine Topologie mit Schleifen, wie sie in Abbildung 20-1 dargestellt ist, kann nützlich und potenziell schädlich sein. Eine Schleife impliziert das Vorhandensein mehrerer Pfade durch das Internetwork. Ein Netzwerk mit mehreren Pfaden von der Quelle bis zum Ziel verfügt über eine so genannte verbesserte topologische Flexibilität, die die Fehlertoleranz des gesamten Netzwerks erhöht.

Der Spanning Tree Algorithmus

Der Spanning-Tree-Algorithmus (STA) wurde von DEC, einem wichtigen Ethernet-Anbieter, entwickelt, um die Vorteile von Schleifen zu erhalten und deren Probleme zu beseitigen. Der DEC-Algorithmus wurde anschließend vom IEEE 802-Ausschuss überarbeitet und in der IEEE 802.1d-Spezifikation veröffentlicht. Der DEC-Algorithmus und der IEEE 802.1d-Algorithmus sind nicht identisch und nicht kompatibel.

Der STA benennt eine schleifenfreie Teilmenge der Topologie des Netzwerks, indem diese Bridge-Ports platziert werden. Wenn diese Ports aktiv sind, kann er Loops in einen Standby-Zustand (Blockierung) erstellen. Die Blockierung des Bridge-Ports kann bei einem Ausfall der primären Verbindung aktiviert werden, wodurch ein neuer Pfad durch das Internet bereitgestellt wird.

Die STA verwendet eine Schlussfolgerung aus der Graphentheorie als Grundlage für den Aufbau einer schleifenfreien Teilmenge der Topologie des Netzes. Die Diagrammtheorie besagt: "Für jedes angeschlossene Diagramm, das aus Knoten und Kanten besteht, die Paar von Knoten verbinden, gibt es einen Spanning Tree aus Kanten, der die Konnektivität des Diagramms aufrecht erhält, jedoch keine Schleifen enthält."

Abbildung 20-2 zeigt, wie der STA Schleifen eliminiert. Die STA ruft an, dass jeder Bridge eine eindeutige Kennung zugewiesen wird. In der Regel ist diese ID eine der MAC-Adressen (Media Access Control) der Bridge sowie eine Prioritätsanzeige. Jedem Port in jeder Bridge wird auch eine eindeutige (innerhalb dieser Bridge) Kennung zugewiesen (in der Regel eine eigene MAC-Adresse). Schließlich ist jeder Bridge-Port mit Pfadkosten verbunden. Die Pfadkosten stellen die Kosten für die Übertragung eines Frames über diesen Port auf ein LAN dar. In Abbildung 20-2 sind die Pfadkosten auf den von jeder Bridge ausgehenden Strecken angegeben. Pfadkosten sind in der Regel Standardwerte, können aber von Netzwerkadministratoren manuell zugewiesen werden.

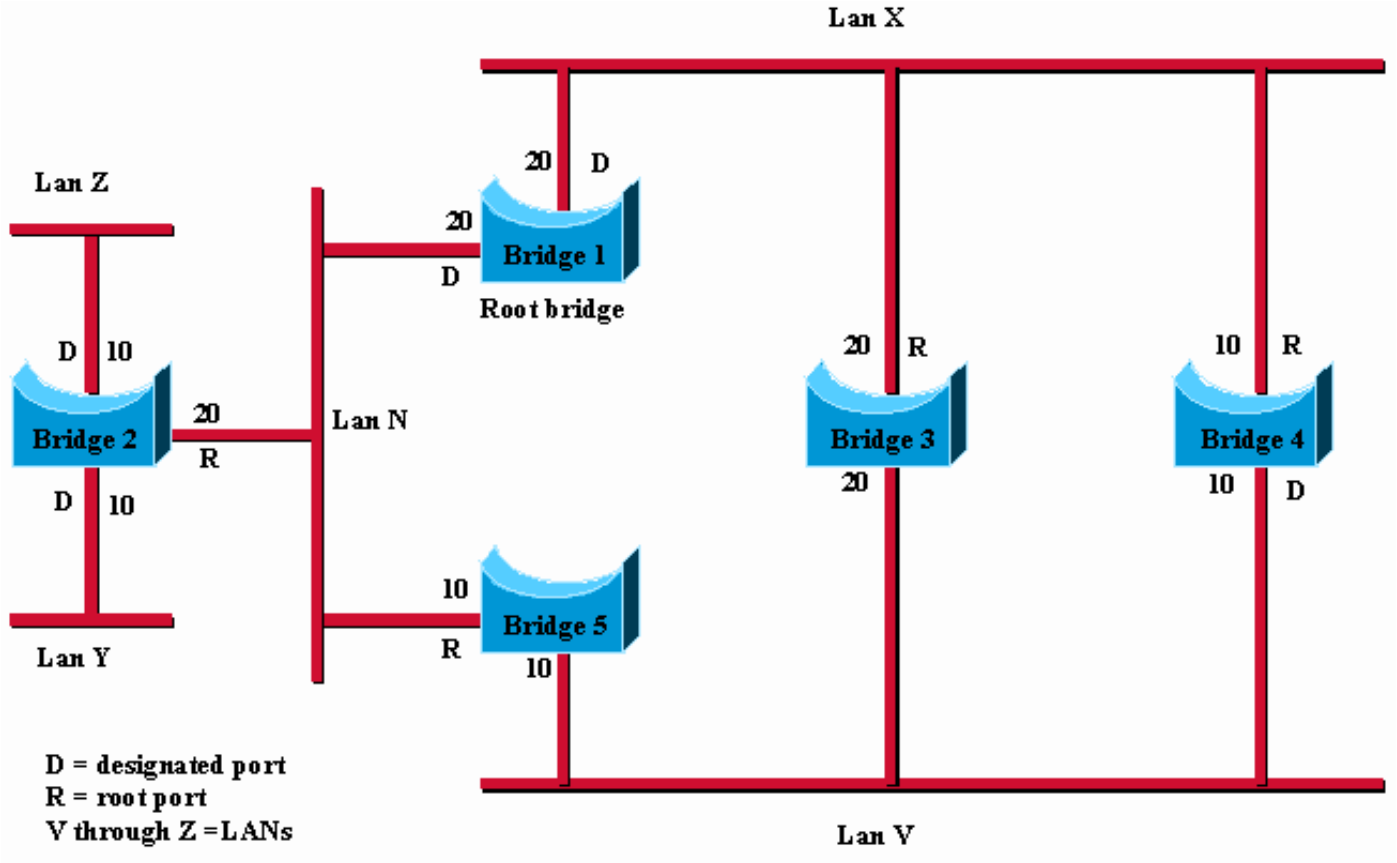


Abbildung 20-2: Transparent Bridge Network (vor STA)

Die erste Aktivität in einer Spanning-Tree-Berechnung ist die Auswahl der Root-Bridge, die die Bridge mit dem niedrigsten Bridge-ID-Wert ist. In Abbildung 20-2 lautet die Root-Bridge Bridge 1. Als Nächstes wird der Root-Port aller anderen Bridges bestimmt. Ein Root-Port einer Bridge ist der Port, über den die Root-Bridge mit den niedrigsten Gesamtkosten für den Pfad erreicht werden kann. Der Wert der geringsten aggregierten Pfadkosten für den Root wird als Root-Pfad-Kosten bezeichnet.

Schließlich werden designierte Bridges und die dafür vorgesehenen Ports festgelegt. Eine designierte Bridge ist die Bridge in jedem LAN, die die Mindestkosten für den Root-Pfad bereitstellt. Eine designierte Bridge eines LANs ist die einzige Bridge, die Frames an das LAN weiterleiten und von diesem trennen darf, für das sie die designierte Bridge ist. Ein designierter Port eines LAN ist der Port, der ihn mit der designierten Bridge verbindet.

In einigen Fällen können zwei oder mehr Bridges die gleichen Root-Pfadkosten verursachen. Beispiel: In Abbildung 20-2 können Bridges 4 und 5 mit Pfadkosten von 10 beide Bridge 1 (die Root Bridge) erreichen. In diesem Fall werden die Bridge-IDs erneut verwendet, um die vorgesehenen Bridges zu ermitteln. Der LAN V-Port von Bridge 4 wird über den LAN V-Port von Bridge 5 ausgewählt.

Bei diesem Vorgang werden alle Brücken außer einer, die direkt mit jedem LAN verbunden sind, eliminiert, wodurch alle zwei LAN-Schleifen entfernt werden. Der STA eliminiert außerdem Schleifen, die mehr als zwei LANs beinhalten, ohne jedoch die Konnektivität zu beeinträchtigen. Abbildung 20-3 zeigt die Ergebnisse aus der Anwendung des STA auf das Netzwerk, wie in Abbildung 20-2 dargestellt. Abbildung 20-2 zeigt die Baumtopologie genauer. Ein Vergleich dieser Abbildung mit Abbildung 20-3 zeigt, dass die STA die Ports für LAN V sowohl in Bridge 3 als auch in Bridge 5 im Standby-Modus platziert hat.

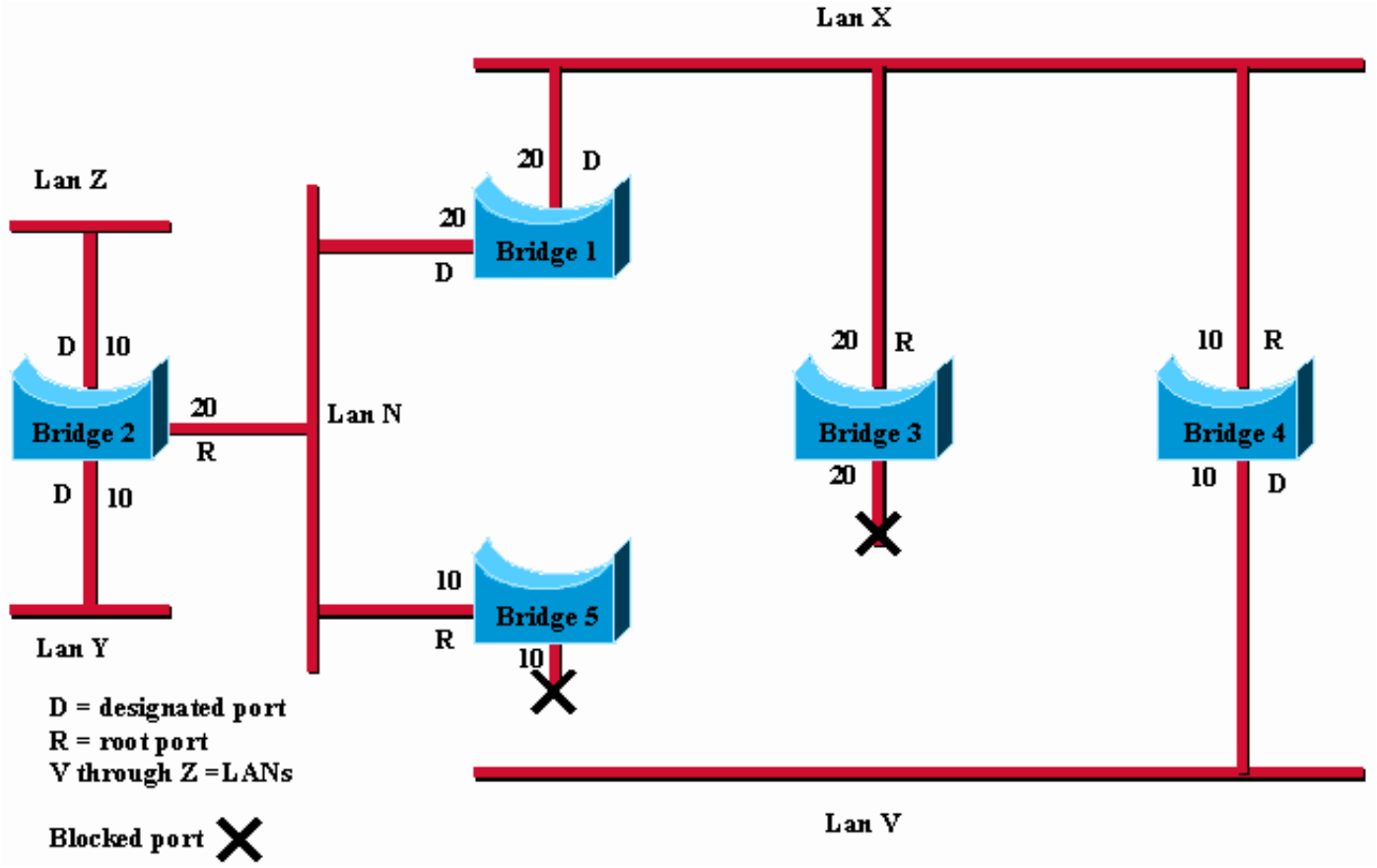


Abbildung 20-3: Transparent Bridge Network (nach STA)

Die Spanning Tree-Berechnung erfolgt beim Einschalten der Bridge und bei jeder Erkennung einer Topologieänderung. Die Berechnung erfordert die Kommunikation zwischen den Spanning Tree Bridges, die über Konfigurationsnachrichten (manchmal auch als Bridge-Protokoll-Dateneinheiten oder BPDUs bezeichnet) erfolgt. Konfigurationsmeldungen enthalten Informationen zur Identifizierung der Bridge, von der angenommen wird, dass sie die Root-Bridge ist (Root-ID), sowie der Entfernung von der sendenden Bridge zur Root-Bridge (Root-Pfad-Kosten). Konfigurationsmeldungen enthalten außerdem die Bridge- und Port-ID der sendenden Bridge und das Alter der in der Konfigurationsmeldung enthaltenen Informationen.

Bridges tauschen in regelmäßigen Abständen Konfigurationsmeldungen aus (in der Regel ein bis vier Sekunden). Wenn eine Bridge ausfällt (was zu einer Topologieänderung führt), erkennen nahegelegene Bridges bald den Mangel an Konfigurationsmeldungen und initiieren eine Neuberechnung des Spanning Tree.

Alle Entscheidungen zur transparenten Bridge-Topologie werden lokal getroffen. Konfigurationsnachrichten werden zwischen nahegelegenen Brücken ausgetauscht. Es gibt keine zentrale Behörde für Netzwerktopologie oder -administration.

Frame-Format

Transparente Bridges tauschen Konfigurationsmeldungen und Meldungen zum Topologiewechsel aus. Konfigurationsmeldungen werden zwischen Bridges gesendet, um eine Netzwerktopologie einzurichten. Meldungen zu Topologieänderungen werden gesendet, nachdem eine Topologieänderung erkannt wurde, um anzuzeigen, dass der STA erneut ausgeführt werden muss.

Tabelle 20-2 zeigt das Konfigurationsmeldungsformat für IEEE 802.1d.

Tabelle 20-2: Transparente Bridge-Konfiguration

Protokollkennung	Version	Meldungstyp	Flags	Root-ID	Root-Path-Kosten	Bridge-ID	Port-ID	Nachrichtenalter	Maximales Alter	Hello-Zeit	Verzögerung der Weiterleitung
2 Byte	1 Byte	1 Byte	1 Byte	8 Byte	4 Byte	8 Byte	2 Byte	2 Byte	2 Byte	2 Byte	2 Byte

Nachrichtenfelder

Transparente Bridge-Konfigurationsmeldungen bestehen aus 35 Byte. Dies sind die Meldungsfelder:

- Protokollkennung: Enthält den Wert 0.
- Version: Enthält den Wert 0.
- Meldungstyp: Enthält den Wert 0.
- Markierung: Ein 1-Byte-Feld, von dem nur die ersten beiden Bit verwendet werden. Das TC-Bit (Topology Change) signalisiert eine Topologieänderung. Das TCA-Bit (Topology Change Bestätigungsbit) wird so eingestellt, dass der Empfang einer Konfigurationsmeldung mit dem TC-Bitsatz bestätigt wird.
- Root-ID: Identifiziert die Root Bridge und listet deren 2-Byte-Priorität auf, gefolgt von ihrer 6-Byte-ID.
- Kosten für Root-Pfad: Enthält die Kosten für den Pfad von der Bridge, die die Konfigurationsmeldung an die Root Bridge sendet.
- Bridge-ID: Identifiziert die Priorität und die ID der Bridge, die die Nachricht sendet.
- Port-ID: Identifiziert den Port, von dem die Konfigurationsmeldung gesendet wurde. In diesem Feld können Schleifen erkannt und bearbeitet werden, die von mehreren angeschlossenen Bridges erstellt wurden.
- Nachrichtenalter: Gibt die verstrichene Zeit an, seit der Root die Konfigurationsmeldung gesendet hat, auf der die aktuelle Konfigurationsmeldung basiert.
- Maximales Alter: Gibt an, wann die aktuelle Konfigurationsmeldung gelöscht werden muss.
- Hello Time: Stellt den Zeitraum zwischen Root Bridge-Konfigurationsmeldungen bereit.
- Verzögerung der Weiterleitung: Stellt die Zeitdauer bereit, die Bridges nach einer Topologieänderung warten müssen, bevor ein Wechsel in einen neuen Zustand erfolgt. Wenn eine Bridge zu schnell wechselt, können nicht alle Netzwerkverbindungen ihren Status ändern, und es können Schleifen entstehen.

Das Format der Meldung zur Topologieänderung ist ähnlich dem der transparenten Bridge-Konfigurationsmeldung, jedoch besteht es nur aus den ersten vier Byte. Dies sind die Meldungsfelder:

- Protokollkennung: Enthält den Wert 0.
- Version: Enthält den Wert 0.
- Meldungstyp: Enthält den Wert 128.

Unterschiedliche IOS-Bridging-Techniken

Cisco Router können auf drei verschiedene Arten Bridging implementieren: Standardverhalten, gleichzeitiges Routing und Bridging (CRB) und integriertes Routing und Bridging (IRB).

Standardverhalten

Bevor IRB- und CRB-Funktionen verfügbar waren, konnten Sie nur ein Protokoll auf Plattformbasis überbrücken oder routen. Das heißt, wenn der Befehl **ip route** verwendet wurde, wurde beispielsweise IP-Routing auf allen Schnittstellen durchgeführt. In dieser Situation konnte die IP-Adresse an keiner der Schnittstellen des Routers überbrückt werden.

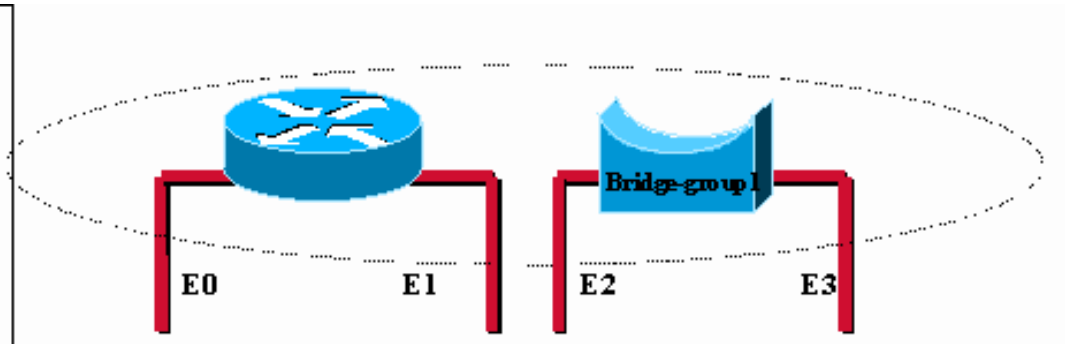
Concurrent Routing and Bridging (CRB)

Mit CRB können Sie bestimmen, ob ein Protokoll auf Schnittstellenbasis überbrückt oder weitergeleitet werden soll. Das heißt, Sie können ein bestimmtes Protokoll auf einigen Schnittstellen routen und dasselbe Protokoll auf Bridge-Group-Schnittstellen innerhalb desselben Routers überbrücken. Der Router kann dann für ein bestimmtes Protokoll sowohl ein Router als

auch eine Bridge sein, aber es kann keine Kommunikation zwischen Routing-definierten Schnittstellen und Bridge-Group-Schnittstellen geben.

Dieses Beispiel veranschaulicht, dass ein einzelner Router für ein bestimmtes Protokoll logisch als separate, unabhängige Geräte agieren kann: ein Router und eine oder mehrere Bridges:

```
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).

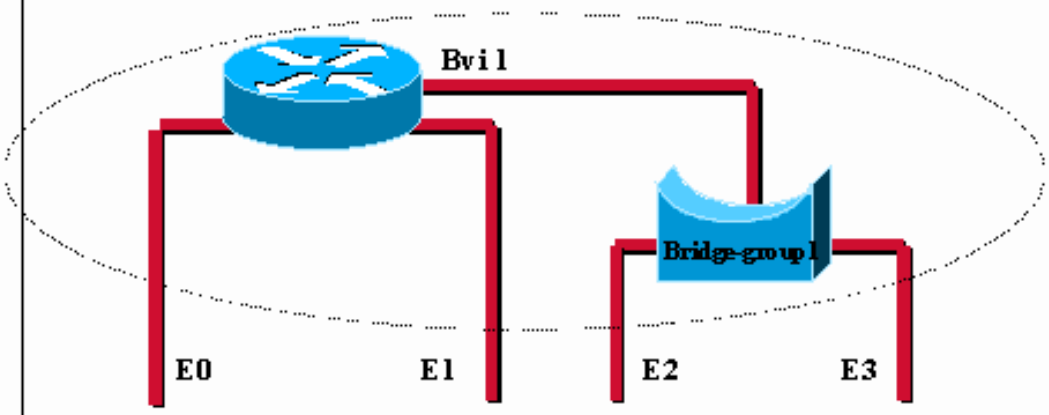
Abbildung 20-4: Concurrent Routing and Bridging (CRB)

Integrated Routing and Bridging (IRB)

IRB bietet die Möglichkeit, zwischen einer Bridge-Gruppe und einer gerouteten Schnittstelle über ein Konzept namens Bridge-Group Virtual Interface (BVI) zu routen. Da das Bridging auf der Sicherungsschicht und dem Routing auf der Netzwerkschicht erfolgt, gibt es verschiedene Protokollkonfigurationsmodelle. Bei IP gehören beispielsweise Bridge-Gruppen-Schnittstellen zum gleichen Netzwerk und haben eine gemeinsame IP-Netzwerkadresse, während jede gerouteten Schnittstelle ein eigenes Netzwerk mit einer eigenen IP-Netzwerkadresse darstellt.

Das BVI-Konzept wurde entwickelt, um diesen Schnittstellen den Austausch von Paketen für ein bestimmtes Protokoll zu ermöglichen. Der Cisco Router sieht, wie in diesem Beispiel gezeigt, wie ein Router aus, der mit einer oder mehreren Bridge-Gruppen verbunden ist:

```
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
```

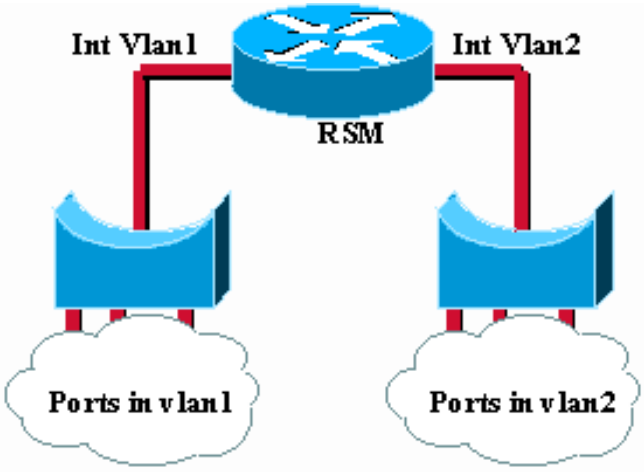


The bridge group virtual interface brings routing to bridge-group 1. One can assign an Ip address to the whole bridge-group and routed communication is now possible between a host connected to E0 and a host connected to E2 for instance.

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

Die BVI ist eine virtuelle Schnittstelle innerhalb des Routers, die wie eine normale geroutete Schnittstelle funktioniert. Die BVI stellt die entsprechende Bridge-Gruppe für geroutete Schnittstellen im Router dar. Die Schnittstellennummer der BVI ist die Nummer der Bridge-Gruppe, die durch diese virtuelle Schnittstelle dargestellt wird. Die Nummer ist die Verbindung zwischen dieser BVI und der Bridge-Gruppe.

In diesem Beispiel wird veranschaulicht, wie das BVI-Prinzip auf das Route Switch Module (RSM) in einem Catalyst Switch angewendet wird:



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).

Abbildung 20-6: Route Switch Module (RSM) in einem Catalyst Switch

Fehlerbehebung: Transparentes Bridging

Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Verbindungsproblemen in transparenten Bridging-Internetworks. Es beschreibt spezifische Symptome für transparente Überbrückungen, die Probleme, die zu jedem Symptom führen können, und die Lösungen für diese Probleme.

Hinweis: Probleme im Zusammenhang mit Source-Route Bridging (SRB), übersetzendem Bridging und Source-Route Transparent (SRT) Bridging werden in Kapitel 10 "Fehlerbehebung bei IBM" behandelt.

Um eine effiziente Fehlerbehebung in Ihrem Bridge-Netzwerk durchführen zu können, benötigen Sie Grundkenntnisse über das Design, insbesondere bei Verwendung eines Spanning Tree.

Diese müssen verfügbar sein:

- Topologieübersicht des Bridge-Netzwerks
- Position der Root Bridge
- Ort der redundanten Verbindung (und blockierter Ports)

Wenn Sie Verbindungsprobleme beheben, reduzieren Sie das Problem auf eine minimale Anzahl von Hosts, idealerweise nur einen Client und einen Server.

In diesen Abschnitten werden die häufigsten Netzwerkprobleme in transparenten, überbrückten Netzwerken beschrieben:

- Transparentes Bridging: Keine Verbindung
- Transparentes Bridging: Instable Spanning Tree
- Transparentes Bridging: Sitzungen werden unerwartet beendet
- Transparentes Bridging: Gewitter mit Schleifen und Senden

Transparentes Bridging: Keine Verbindung

Symptom: Der Client kann über ein transparent überbrücktes Netzwerk keine Verbindung zu Hosts herstellen.

In Tabelle 20-3 sind die Probleme aufgeführt, die dieses Symptom verursachen können, und es werden Lösungen vorgeschlagen.

Tabelle 20-3: Transparentes Bridging: Keine Verbindung

Mögliche Ursachen	Empfohlene Aktionen
Hardware- oder Medienproblem	1. Verwenden Sie den Befehl **show bridge** EXEC, um festzustellen, ob ein Verbindungsproblem vorliegt. In diesem Fall werden in der Ausgabe keine MAC[1]-Adressen in der Bridging-Tabelle angezeigt. 2. Bestimmen Sie mithilfe des Befehls show interfaces EXEC, ob die Schnittstelle und das Leitungsprotokoll aktiv sind.

	3. Wenn die Schnittstelle ausgefallen ist, führen Sie eine Fehlerbehebung für die Hardware oder die Medien durch. Siehe Kapitel 3, "Fehlerbehebung bei Hardware- und Startproblemen". 4. Wenn das Verbindungsprotokoll ausgefallen ist, überprüfen Sie die physische Verbindung zwischen der Schnittstelle und dem Netzwerk. Stellen Sie sicher, dass die Verbindung sicher ist und dass die Kabel nicht beschädigt sind. Wenn das Leitungsprotokoll aktiv ist, die Eingabe- und Ausgabepaketzähler jedoch nicht inkrementiert werden, überprüfen Sie die Medien- und Hostverbindung. Im Kapitel zur Fehlerbehebung für Medien wird der in Ihrem Netzwerk verwendete Medientyp beschrieben.
Host ist ausgefallen	1. Verwenden Sie den Befehl **show bridge** EXEC auf Bridges, um sicherzustellen, dass die Bridging-Tabelle die MAC-Adressen der angeschlossenen Endknoten enthält. Die Bridging-Tabelle enthält die Quell- und Ziel-MAC-Adressen der Hosts und wird gefüllt, wenn Pakete von einer Quelle oder einem Ziel über die Bridge übertragen werden. 2. Wenn erwartete Endknoten fehlen, überprüfen Sie den Status der Knoten, um sicherzustellen, dass sie angeschlossen und ordnungsgemäß konfiguriert sind. 3. Reinitialisieren oder rekonfigurieren Sie bei Bedarf Endknoten, und überprüfen Sie die Bridging-Tabelle mit dem Befehl **show bridge**.
Bridging-Pfad ist defekt	1. Identifizieren Sie den Pfad, über den Pakete zwischen Endknoten übertragen werden müssen. Wenn auf diesem Pfad ein Router vorhanden ist, teilen Sie die Fehlerbehebung in zwei Teile: Knoten 1-Router und Router-Knoten 2. 2. Stellen Sie eine Verbindung zu jeder Bridge auf dem Pfad her, und überprüfen Sie den Status der Ports,

	die auf dem Pfad zwischen den Endknoten verwendet werden (wie im Tabelleneintrag "Hardware- oder Medienproblem" beschrieben). 3. Mit dem Befehl **show bridge** können Sie sicherstellen, dass die MAC-Adresse der Knoten auf den richtigen Ports abgerufen wird. Andernfalls kann es zu Instabilitäten in der Spanning-Tree-Topologie kommen. Siehe Tabelle 20-2, "Transparent Bridging: Unstable Spanning Tree." 4. Überprüfen Sie den Status der Ports mit dem Befehl **show span**. Wenn sich die Ports, die Datenverkehr zwischen den Endknoten übertragen können, nicht im Weiterleitungsstatus befinden, kann sich die Topologie Ihres Trees unerwartet geändert haben. Siehe Tabelle 20-4, "Transparent Bridging Unstable Spanning Tree".
Fehlkonfigurierte Bridging-Filter	1. Mit dem Befehl **show running-config** des privilegierten EXEC-Modus können Sie bestimmen, ob Bridge-Filter konfiguriert sind. 2. Deaktivieren Sie Bridge-Filter an verdächtigen Schnittstellen, und bestimmen Sie, ob die Verbindung wiederhergestellt wird. 3. Wenn die Verbindung nicht wiederhergestellt wird, ist der Filter nicht das Problem. Wenn die Verbindung wiederhergestellt wird, nachdem Filter entfernt wurden, sind ein oder mehrere schädliche Filter die Ursache des Verbindungsproblems. 4. Wenn entweder mehrere Filter vorhanden sind oder Filter, die Zugriffslisten mit mehreren Anweisungen verwenden, wenden Sie jeden Filter einzeln an, um den Problemfilter zu identifizieren. Prüfen Sie die Konfiguration auf **LSAP**[2]- und **TYPE-**Filter, die gleichzeitig zum Blockieren verschiedener Protokolle verwendet werden können.

	Beispielsweise kann **LSAP (F0F0)** zum Blockieren von NetBIOS und **TYPE (6004)** zum Blockieren von Nahbereichsübertragungen verwendet werden. 5. Ändern Sie alle Filter oder Zugriffslisten, die Datenverkehr blockieren. Testen Sie weiterhin die Filter, bis alle Filter aktiviert sind und die Verbindungen weiterhin funktionieren.
Eingabe- und Ausgabewarteschlangen voll	Ein zu hoher Multicast- oder Broadcast-Datenverkehr kann zu einem Überlauf der Ein- und Ausgabewarteschlangen führen, der zu Paketverlusten führt. 1. Suchen Sie mit dem Befehl **show interfaces** nach Eingabe- und Ausgabeverwerfungen. Drops deuten auf übermäßigen Datenverkehr über die Medien hin. Wenn die aktuelle Anzahl der Pakete in der Eingangswarteschlange konsistent 80 % oder mehr der aktuellen Größe der Eingangswarteschlange beträgt, muss die Größe der Eingangswarteschlange angepasst werden, um die Paketrate anzupassen. Selbst wenn die aktuelle Anzahl der Pakete in der Eingangswarteschlange nie der Größe der Eingangswarteschlange nähert, können die Paketspitzen die Warteschlange weiterhin überlaufen. 2. Verringern Sie den Broadcast- und Multicast-Datenverkehr in angeschlossenen Netzwerken mithilfe von Bridging-Filtern, oder segmentieren Sie das Netzwerk mit mehr Internetgeräten. 3. Wenn es sich bei der Verbindung um eine serielle Verbindung handelt, erhöhen Sie die Bandbreite, wenden Prioritätswarteschlangen an, erhöhen die Größe der Warteschlange oder ändern Sie die Größe des Systempuffers. Weitere Informationen finden Sie in Kapitel 15,

	"Fehlerbehebung bei Problemen mit der seriellen Leitung".

[1]MAC = Media Access Control

[2]LSAP = Link Services Access Point

Transparentes Bridging: Instable Spanning Tree

Symptom: Transparenter Verbindungsverlust zwischen Hosts Mehrere Hosts sind gleichzeitig betroffen.

In Tabelle 20-4 sind die Probleme aufgeführt, die dieses Symptom verursachen können, und es werden Lösungen vorgeschlagen.

Tabelle 20-4: Transparentes Bridging: Instable Spanning Tree

Mögliche Ursachen	Empfohlene Aktionen
Link-Flapping	1. Mit dem Befehl **show span** können Sie feststellen, ob die Anzahl der Topologien stetig zunimmt. 2. Wenn ja, überprüfen Sie die Verbindung zwischen Ihren Bridges mit dem Befehl **show interface**. Wenn dieser Befehl keine Verbindungsflapping zwischen zwei Brücken aufdeckt, verwenden Sie den Befehl **debug spantree event** privileged EXEC auf Ihren Bridges. Dadurch werden alle Änderungen im Zusammenhang mit dem Spanning Tree protokolliert. In einer stabilen Topologie kann es keine geben. Die einzigen Links, die zur Spur führen, sind diejenigen, die die Bridge-Geräte miteinander verbinden. Ein Übergang auf eine Verbindung zu einer Endstation sollte keine Auswirkungen auf das Netzwerk haben. **Hinweis:** Da der Debug-Ausgabe im CPU-Prozess eine hohe Priorität zugewiesen wird, kann die Verwendung des Befehls **debug spantree event** das System unbrauchbar machen. Verwenden Sie deshalb nur **Debug-**Befehle, um spezifische Probleme zu beheben, oder wenn Sie in Sitzungen Probleme mit dem technischen Support von Cisco beheben. Darüber hinaus ist es am besten, **Debugbefehle** innerhalb von Zeiträumen zu verwenden, in denen der Netzwerkverkehr gering ist und

	weniger Benutzer erforderlich sind. Wenn Sie das Debuggen innerhalb dieser Zeiträume durchführen, verringert dies die Wahrscheinlichkeit, dass sich die Systemnutzung durch erhöhte Prozesse **für** den **Debugging-**Befehlsoverhead beeinträchtigt.
Root Bridge ändert sich weiter; mehrere Bridges behaupten, der Root-Bridge zu sein.	1. Prüfen Sie die Konsistenz der Root Bridge-Informationen im gesamten Bridge-Netzwerk mithilfe der **show span-**Befehle auf den verschiedenen Bridges. 2. Wenn es mehrere Bridges gibt, die den Root angeben, stellen Sie sicher, dass Sie dasselbe Spanning Tree-Protokoll auf jeder Bridge ausführen (siehe Tabelleneintrag "Spanning Tree Algorithmus Mismatch" in Tabelle 20-6). 3. Verwenden Sie den Befehl **bridge** *<group>* priority*<number>* auf der Root-Bridge, um die gewünschte Bridge zum Root-Bridge zu zwingen. Je niedriger die Priorität, desto wahrscheinlicher ist es, dass die Bridge die Root wird. 4. Überprüfen Sie den Netzwerkdurchmesser. Wenn ein standardmäßiger Spanning Tree eingerichtet ist, darf es zwischen zwei Hosts nie mehr als sieben Bridge-Hops geben.
Hellos nicht ausgetauscht	1. Überprüfen Sie, ob Bridges miteinander kommunizieren. Verwenden Sie einen Netzwerkanalyzer oder den Befehl **debug spantree** privilegierter EXEC, um festzustellen, ob Spanning Tree Hello-Frames ausgetauscht werden. **Hinweis:** Da der Debug-Ausgabe im CPU-Prozess eine hohe Priorität zugewiesen wird, kann die Verwendung des Befehls **debug spantree event** das System unbrauchbar machen. Verwenden Sie deshalb nur **Debug-**Befehle, um spezifische Probleme zu beheben, oder wenn Sie in Sitzungen Probleme mit dem technischen Support von Cisco beheben. Darüber hinaus ist es am besten, **Debugbefehle** innerhalb von Zeiträumen zu verwenden, in denen der Netzwerkverkehr gering ist und weniger Benutzer erforderlich sind. Wenn Sie das Debuggen innerhalb dieser Zeiträume durchführen, verringert dies die

	Wahrscheinlichkeit, dass sich die Systemnutzung durch erhöhte Prozesse für den Debugging-Befehlsoverhead beeinträchtigt. 2. Wenn Hellos nicht ausgetauscht werden, überprüfen Sie die physischen Verbindungen und die Softwarekonfiguration auf den Bridges.

Transparentes Bridging: Sitzungen werden unerwartet beendet

Symptom: Verbindungen in einer transparent überbrückten Umgebung werden erfolgreich hergestellt, Sitzungen werden jedoch manchmal abrupt beendet.

In Tabelle 20-5 sind die Probleme aufgeführt, die dieses Symptom verursachen können, und es werden Lösungen vorgeschlagen.

Tabelle 20-5: Transparentes Bridging: Sitzungen werden unerwartet beendet

Mögliche Ursachen	Empfohlene Aktionen
Übermäßige Neuübertragungen	1. Suchen Sie mithilfe eines Netzwerkanalysetools nach Neuübertragungen von Hosts. 2. Wenn Sie bei langsamen seriellen Leitungen Wiederübertragungen sehen, erhöhen Sie die Übertragungstimer auf dem Host. Weitere Informationen zum Konfigurieren der Hosts finden Sie in der Dokumentation des Herstellers. Weitere Informationen zur Fehlerbehebung bei seriellen Posten finden Sie in Kapitel 15, "Fehlerbehebung bei Problemen mit der seriellen Leitung". Wenn Sie auf Hochgeschwindigkeits-LAN-Medien Neuübertragungen sehen, überprüfen Sie, ob Pakete in der richtigen Reihenfolge gesendet und empfangen oder von einem zwischengeschalteten Gerät (z. B. einer Bridge oder einem Switch) verworfen wurden. Fehlerbehebung bei LAN-Medien nach Bedarf Weitere Informationen finden Sie im Kapitel zur Fehlerbehebung bei Medien, die den in Ihrem Netzwerk verwendeten Medientyp abdecken. 3. Bestimmen Sie mithilfe eines Netzwerkanalysetools, ob die Anzahl der

	erneuten Übertragungen weitergeleitet wird.
Übermäßige Verzögerung bei serieller Verbindung	Erhöhen Sie die Bandbreite, wenden Sie Prioritätswarteschlangen an, erhöhen Sie die Größe der Warteschlange, oder ändern Sie die Größe des Systempuffers. Weitere Informationen finden Sie in Kapitel 15, "Fehlerbehebung bei Problemen mit der seriellen Leitung".

Transparentes Bridging: Gewitter mit Schleifen und Senden

Symptom: Paketschleifen und Broadcast-Stürme treten in transparenten Bridge-Umgebungen auf. Endstationen werden zu einer übermäßigen Neuübertragung gezwungen, wodurch Sitzungen zeitgesteuert oder abgebrochen werden.

Hinweis: Paketschleifen werden in der Regel durch Probleme mit dem Netzwerkdesign oder Hardware verursacht.

In Tabelle 20-6 sind die Probleme aufgeführt, die dieses Symptom verursachen können, und es werden Lösungen vorgeschlagen.

Bridging-Loops sind das Worst-Case-Szenario in einem überbrückten Netzwerk, da sie potenziell alle Benutzer betreffen können. Im Notfall können Sie die Konnektivität am besten durch eine manuelle Deaktivierung aller Schnittstellen wiederherstellen, die einen redundanten Pfad im Netzwerk bereitstellen. Leider wird die Ursache der Bridging-Schleife im Nachhinein sehr schwer zu identifizieren sein, wenn Sie dies tun. Wenn möglich, sollten Sie die Aktionen in Tabelle 20-6 im Voraus ausprobieren.

Tabelle 20-6: Transparentes Bridging: Gewitter mit Schleifen und Senden

Mögliche Ursachen	Empfohlene Aktionen
Kein Spanning Tree implementiert	1. Prüfen Sie eine Topologieübersicht Ihres Internetworks, um mögliche Schleifen zu finden. 2. Beseitigen Sie alle vorhandenen Schleifen, oder stellen Sie sicher, dass sich die entsprechenden Links im Backup-Modus befinden. 3. Wenn Broadcast-Stürme und Paket-Schleifen anhalten, können Sie mit dem Befehl **show interfaces** EXEC Statistiken zur Eingabe- und Ausgabe-Paketanzahl abrufen. Wenn diese Zähler mit einer ungewöhnlich hohen Rate inkrementieren (in Bezug auf Ihre normalen Datenverkehrslasten), ist im Netzwerk

	wahrscheinlich noch eine Schleife vorhanden. 4. Implementieren Sie einen Spanning Tree-Algorithmus, um Schleifen zu vermeiden.
Nichtübereinstimmung des Spanning Tree-Algorithmus	1. Bestimmen Sie mithilfe des Befehls **show span** EXEC auf jeder Bridge, welcher Spanning Tree-Algorithmus verwendet wird. 2. Stellen Sie sicher, dass alle Bridges denselben Spanning Tree-Algorithmus ausführen (entweder DEC oder IEEE)[1]. Es kann erforderlich sein, sowohl die Spanning Tree-Algorithmen DEC als auch IEEE für einige sehr spezifische Konfigurationen im Netzwerk zu verwenden (in der Regel diejenigen, die IRB beinhalten). Wenn die Abweichung im Spanning Tree-Protokoll nicht beabsichtigt ist, müssen die Bridges entsprechend neu konfiguriert werden, sodass alle Bridges denselben Spanning Tree-Algorithmus verwenden. **Hinweis:** Die DEC- und IEEE-Spanning-Tree-Algorithmen sind nicht kompatibel.
Mehrere Bridging-Domänen falsch konfiguriert	1. Verwenden Sie den Befehl **show span** EXEC auf Bridges, um sicherzustellen, dass alle Domänengruppen-Nummern mit den angegebenen Bridging-Domänen übereinstimmen. 2. Wenn mehrere Domänengruppen für die Bridge konfiguriert sind, stellen Sie sicher, dass alle Domänenspezifikationen korrekt zugewiesen sind. Mit dem Befehl **bridge** *<group>***domain** *<domain-number>* global configuration können Sie erforderliche Änderungen vornehmen. 3. Stellen Sie sicher, dass zwischen Bridging-Domänen keine Schleifen vorhanden sind. Eine Interdomain-Bridging-Umgebung bietet keine auf Spanning Tree basierende

	Schleifenvermeidung. Jede Domäne verfügt über einen eigenen Spanning Tree, der unabhängig vom Spanning Tree in anderen Domänen ist.
Verbindungsfehler (unidirektionale Verbindung), Duplexungleichheit, hohe Fehlerrate an einem Port.	Schleifen treten auf, wenn ein Port, der den Weiterleitungsstatus blockieren soll, in den Weiterleitungsstatus verschoben wird. Ein Port muss BPDUs von einer nahegelegenen Bridge empfangen, um im Blockierungsstatus zu bleiben. Jeder Fehler, der zu verlorenen BPDUs führt, kann dann die Ursache einer Bridging-Schleife sein. 1. Identifizieren Sie blockierende Ports aus Ihrem Netzwerkdiagramm. 2. Überprüfen Sie den Status der Ports, die in Ihrem Bridge-Netzwerk mit der **Show-Schnittstelle** blockiert werden sollen, und **zeigen Sie Bridge-**EXEC-Befehle an. 3. Wenn Sie einen möglicherweise blockierten Port finden, der derzeit weiterleitet oder weitergeleitet wird (d. h. im Lern- oder Hörstatus), haben Sie die eigentliche Ursache des Problems gefunden. Überprüfen Sie, ob dieser Port BPDUs empfängt. Wenn nicht, besteht wahrscheinlich ein Problem mit dem Link, der mit diesem Port verbunden ist. Überprüfen Sie dann Verbindungsfehler, Duplexeinstellungen usw.). Wenn der Port immer noch BPDUs empfängt, gehen Sie zu der Bridge, von der Sie erwarten, dass sie für dieses LAN designiert ist. Überprüfen Sie dann alle Links auf dem Pfad zum Root. Unter einem dieser Links finden Sie ein Problem (vorausgesetzt, dass Ihr anfängliches Netzwerkdiagramm korrekt war).

[1]IEEE = Institute of Electrical and Electronic Engineers

Bevor Sie das Cisco Systems TAC Team anrufen

Wenn Ihr Netzwerk stabil ist, sammeln Sie so viele Informationen wie möglich über die Topologie.

Sammeln Sie mindestens diese Daten:

- Physische Topologie des Netzwerks
- Erwarteter Standort der Root-Bridge (und Backup-Root-Bridge)
- Position blockierter Ports

Weitere Quellen

Bücher:

- Verbindungen, Bridges und Router, Radia Perlman, Addison-Wesley
- Cisco LAN Switching, K.Clark, K.Hamilton, Cisco Press

Zugehörige Informationen

- Transparent Bridging-Dokumentation
- Technischer Support und Dokumentation für Cisco Systeme