Risoluzione dei problemi relativi agli ambienti di bridging trasparenti

Sommario

Obiettivi

I bridge trasparenti sono stati sviluppati per la prima volta dalla Digital Equipment Corporation (DEC) nei primi anni '80 e sono ora molto diffusi nelle reti Ethernet/IEEE 802.3'.

- In questo capitolo viene innanzitutto definito un bridge trasparente come un learning bridge che implementa il protocollo Spanning Tree. Include una descrizione dettagliata del protocollo Spanning Tree.
- I dispositivi Cisco che implementano bridge trasparenti erano suddivisi in due categorie: router con software Cisco IOS® e la gamma di switch Catalyst con software specifico. Non è più così. Diversi prodotti Catalyst sono ora basati su IOS. In questo capitolo vengono descritte le diverse tecniche di bridging disponibili per i dispositivi IOS. Per la configurazione e la risoluzione dei problemi specifici del software Catalyst, fare riferimento al capitolo sullo switching LAN.
- Infine, vengono introdotte alcune procedure di risoluzione dei problemi che vengono classificate in base ai sintomi di problemi potenziali che in genere si verificano in reti di bridging trasparenti.

Nozioni di base sulla tecnologia Transparent Bridging

Il nome dei bridge trasparenti deriva dal fatto che la loro presenza e il loro funzionamento sono trasparenti per gli host di rete. Quando i bridge trasparenti sono accesi, imparano la topologia della rete analizzando l'indirizzo di origine dei frame in ingresso da tutte le reti collegate. Se, ad esempio, un bridge vede arrivare un frame sulla linea 1 dall'host A, conclude che l'host A può essere raggiunto attraverso la rete connessa alla linea 1. Tramite questo processo, i bridge trasparenti creano una tabella di bridging interna come quella della tabella 20-1.

Tabella 20-1: Tabella di raccordo trasparente

Indirizzo host	Numero di rete
0000.0000.0001	1
0000.b07e.ee0e	7
?	-
0050.50e1.9b80	4
0060.b0d9.2e3d	2
0000.0c8c.7088	1
?	-

Il bridge utilizza la tabella di bridging come base per l'inoltro del traffico. Quando si riceve un frame su una delle interfacce bridge, il bridge cerca l'indirizzo di destinazione del frame nella relativa tabella interna. Se la tabella è mappata tra l'indirizzo di destinazione e una delle porte del bridge (a parte quella in cui il frame è stato ricevuto), il frame viene inoltrato alla porta specificata. Se non viene trovata alcuna mappa, il frame viene esteso a tutte le porte in uscita. In questo modo vengono inondate anche le trasmissioni radiotelevisive e i multicast.

I bridge trasparenti riescono a isolare il traffico all'interno dei segmenti e a ridurre il traffico rilevato su ogni singolo segmento. In questo modo vengono in genere migliorati i tempi di risposta della rete. La riduzione del traffico e il miglioramento dei tempi di risposta dipendono dal volume del traffico tra segmenti (in rapporto al traffico totale), nonché dal volume del traffico broadcast e multicast.

Bridging di loop

Senza un protocollo bridge-to-bridge, l'algoritmo del bridge trasparente ha esito negativo quando vi sono più percorsi di bridge e reti LAN (Local Area Network) tra due LAN qualsiasi nell'internetwork. La Figura 20-1 illustra un tale ciclo di bridging.

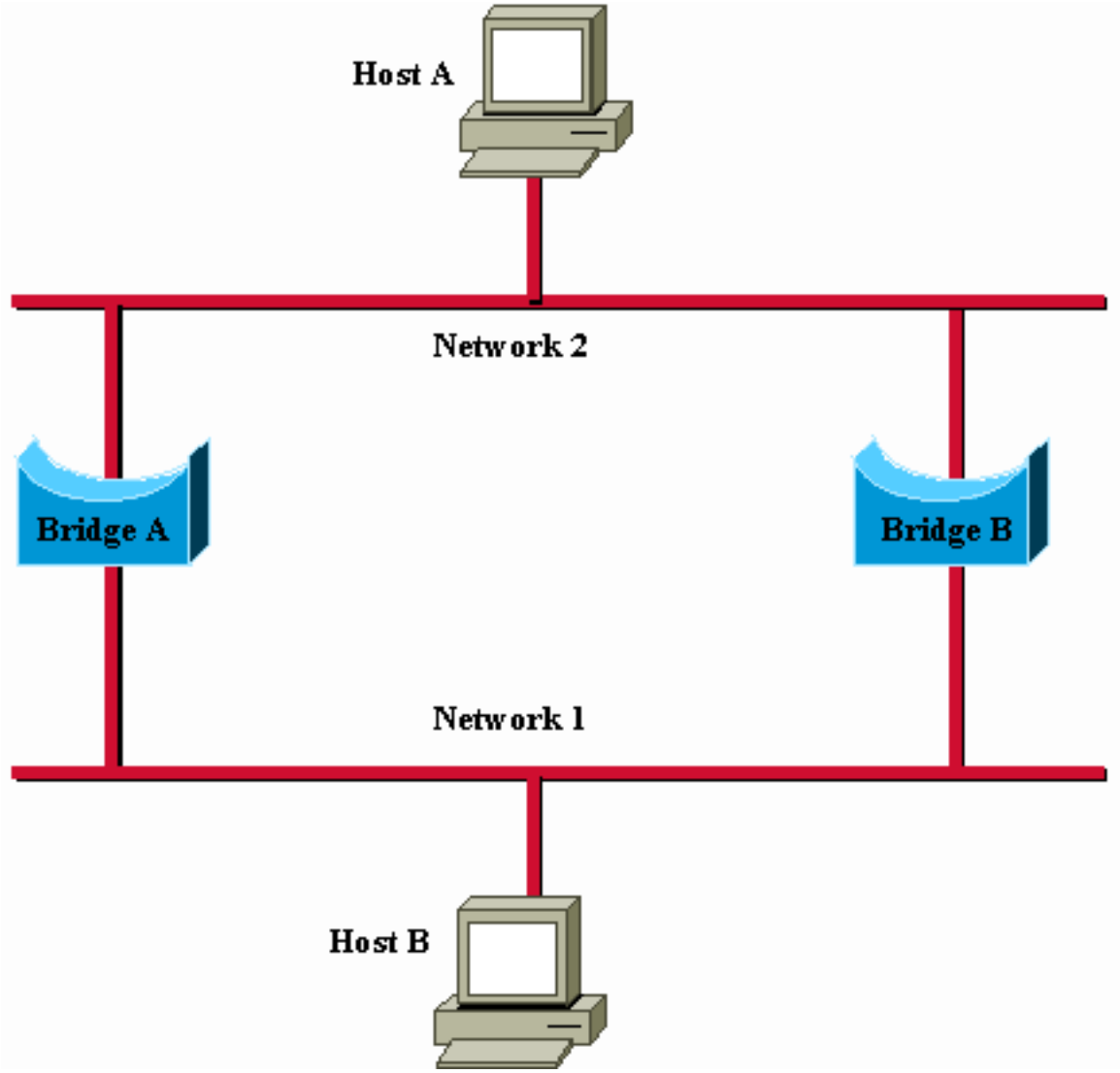


Figura 20-1: Inoltro e apprendimento imprecisi in ambienti di bridging trasparenti

Si supponga che l'host A invii un frame all'host B. Entrambi i bridge ricevono il frame e concludono correttamente che l'host A è sulla rete 2. Purtroppo, dopo la ricezione di due copie del frame dell'host A, entrambi i bridge ricevono nuovamente il frame sulla propria interfaccia di rete 1 perché tutti gli host ricevono tutti i messaggi sulle LAN di trasmissione. In alcuni casi, i bridge modificheranno quindi le proprie tabelle interne per indicare che l'host A si trova sulla rete 1. In questo caso, quando l'host B risponde al frame dell'host A, entrambi i bridge ricevono e quindi eliminano le risposte perché le rispettive tabelle indicano che la destinazione (host A) si trova sullo stesso segmento di rete dell'origine del frame.

Oltre ai problemi di connettività di base, come quello descritto, la proliferazione dei messaggi broadcast su reti con loop rappresenta un problema di rete potenzialmente serio. In riferimento alla Figura 20-1, si supponga che il frame iniziale dell'host A sia una trasmissione. Entrambi i bridge inoltrano i frame in modo continuo, utilizzano tutta la larghezza di banda disponibile e bloccano la trasmissione di altri pacchetti su entrambi i segmenti.

Una topologia con loop come quella illustrata nella Figura 20-1 può essere utile e potenzialmente dannosa. Un loop implica l'esistenza di più percorsi attraverso la rete interna. Una rete con più percorsi dall'origine alla destinazione presenta una maggiore flessibilità topologica che aumenta la tolleranza di errore globale della rete.

Algoritmo Spanning Tree

Lo Spanning Tree Algorithm (STA) è stato sviluppato da DEC, un fornitore chiave di Ethernet, per preservare i vantaggi dei loop ed eliminare al contempo i loro problemi. L'algoritmo DEC è stato successivamente revisionato dal comitato IEEE 802 e pubblicato nella specifica IEEE 802.1d. L'algoritmo DEC e l'algoritmo IEEE 802.1d non sono uguali né compatibili.

La STA designa un sottoinsieme senza loop della topologia della rete mediante il posizionamento di tali porte bridge, in modo che, se attiva, possa creare loop in una condizione di standby (blocco). Il blocco delle porte del bridge può essere attivato in caso di errore del collegamento primario, che fornisce un nuovo percorso attraverso la rete interna.

La STA utilizza una conclusione della teoria dei grafi come base per la costruzione di un sottoinsieme privo di loop della topologia della rete. La teoria dei grafici afferma: "Per ogni grafico connesso costituito da nodi e spigoli che collegano coppie di nodi, esiste un albero di spanning di spigoli che mantiene la connettività del grafico ma non contiene loop."

La Figura 20-2 illustra come la STA elimina i loop. La STA richiede che a ogni bridge venga assegnato un identificatore univoco. In genere, questo identificatore è uno degli indirizzi MAC (Media Access Control) del bridge più un'indicazione di priorità. A ogni porta di ogni bridge viene inoltre assegnato un identificatore univoco, all'interno del bridge, in genere il relativo indirizzo MAC. Infine, a ciascuna porta bridge è associato un costo del percorso. Il costo del percorso rappresenta il costo della trasmissione di un frame su una LAN attraverso quella porta. Nella Figura 20-2, i costi dei percorsi sono riportati sulle linee che provengono da ciascun ponte. I costi dei percorsi sono in genere valori predefiniti, ma possono essere assegnati manualmente dagli amministratori di rete.

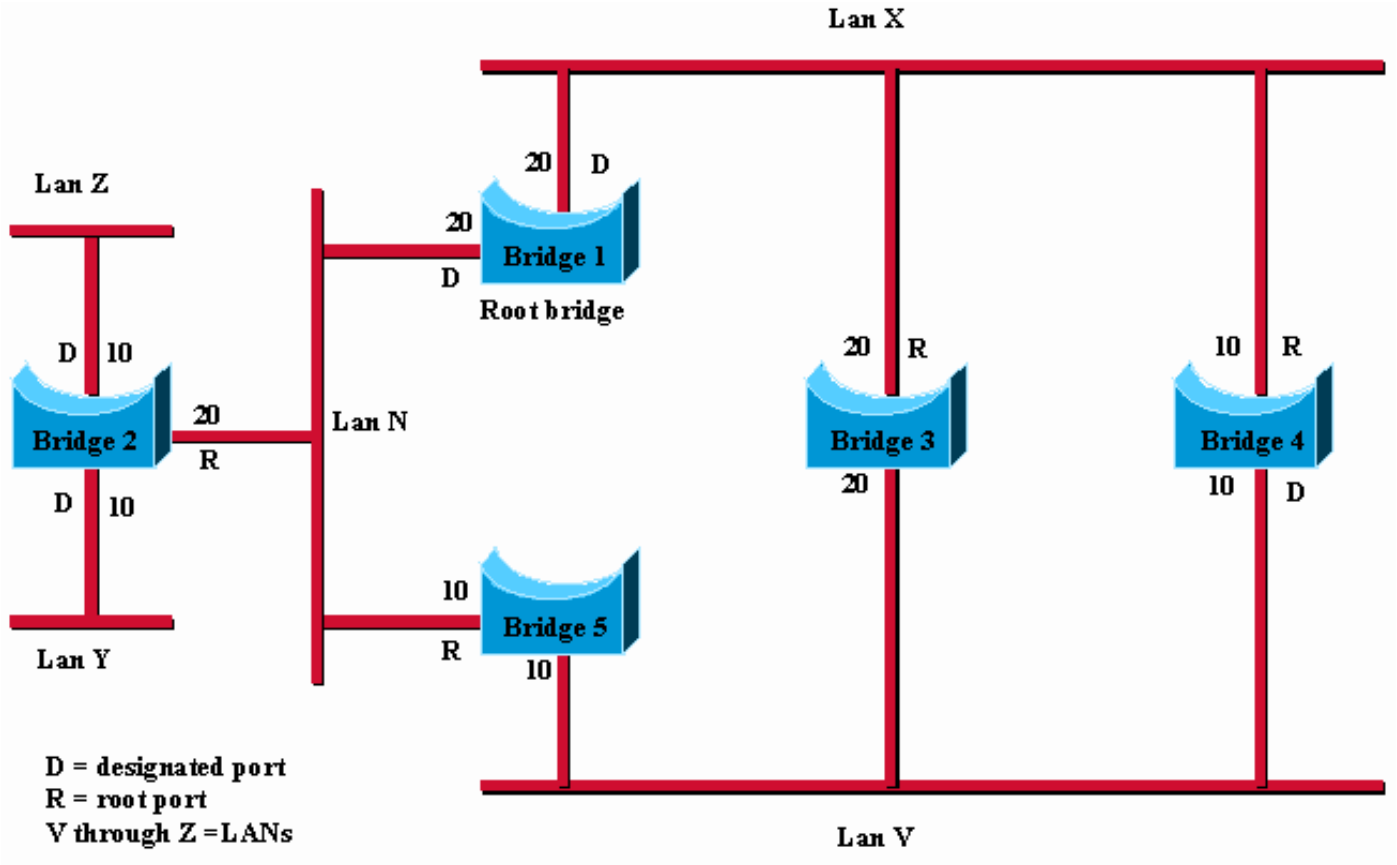


Figura 20-2: Rete bridge trasparente (prima di STA)

La prima attività in un calcolo Spanning Tree è la selezione del bridge radice, ovvero il bridge con il valore identificativo del bridge più basso. Nella Figura 20-2, il ponte principale è il Ponte 1. Successivamente, viene determinata la porta principale su tutti gli altri ponti. Una porta radice di

un bridge è la porta attraverso la quale il bridge radice può essere raggiunto con il minor costo aggregato di percorso. Il valore del costo del percorso meno aggregato per la radice è detto costo del percorso radice.

Infine, vengono determinati i ponti designati e i relativi porti designati. Un bridge designato è il bridge su ciascuna LAN che fornisce il costo minimo del percorso radice. Un bridge designato di una LAN è l'unico bridge autorizzato a inoltrare i frame da e verso la LAN per cui rappresenta il bridge designato. Una porta designata di una LAN è la porta che la connette al bridge designato.

In alcuni casi, due o più bridge possono avere lo stesso costo per il percorso radice. Ad esempio, nella Figura 20-2, i ponti 4 e 5 possono entrambi raggiungere il ponte 1 (il ponte principale) con un costo del percorso di 10. In questo caso, gli identificativi del ponte vengono utilizzati nuovamente, questa volta, per determinare i ponti designati. La porta LAN V del bridge 4 è selezionata sulla porta LAN V del bridge 5.

Con questo processo, vengono eliminati tutti i bridge ad eccezione di uno direttamente collegati a ciascuna LAN, rimuovendo tutti i loop tra due LAN. La STA elimina anche i loop che coinvolgono più di due LAN, pur preservando la connettività. La Figura 20-3 mostra i risultati dell'applicazione della STA alla rete mostrati nella Figura 20-2. La Figura 20-2 mostra la topologia della struttura in modo più chiaro. Un confronto tra questa figura e la Figura 20-3 mostra che la STA ha posizionato le porte sulla LAN V sia in Bridge 3 che in Bridge 5 in modalità standby.

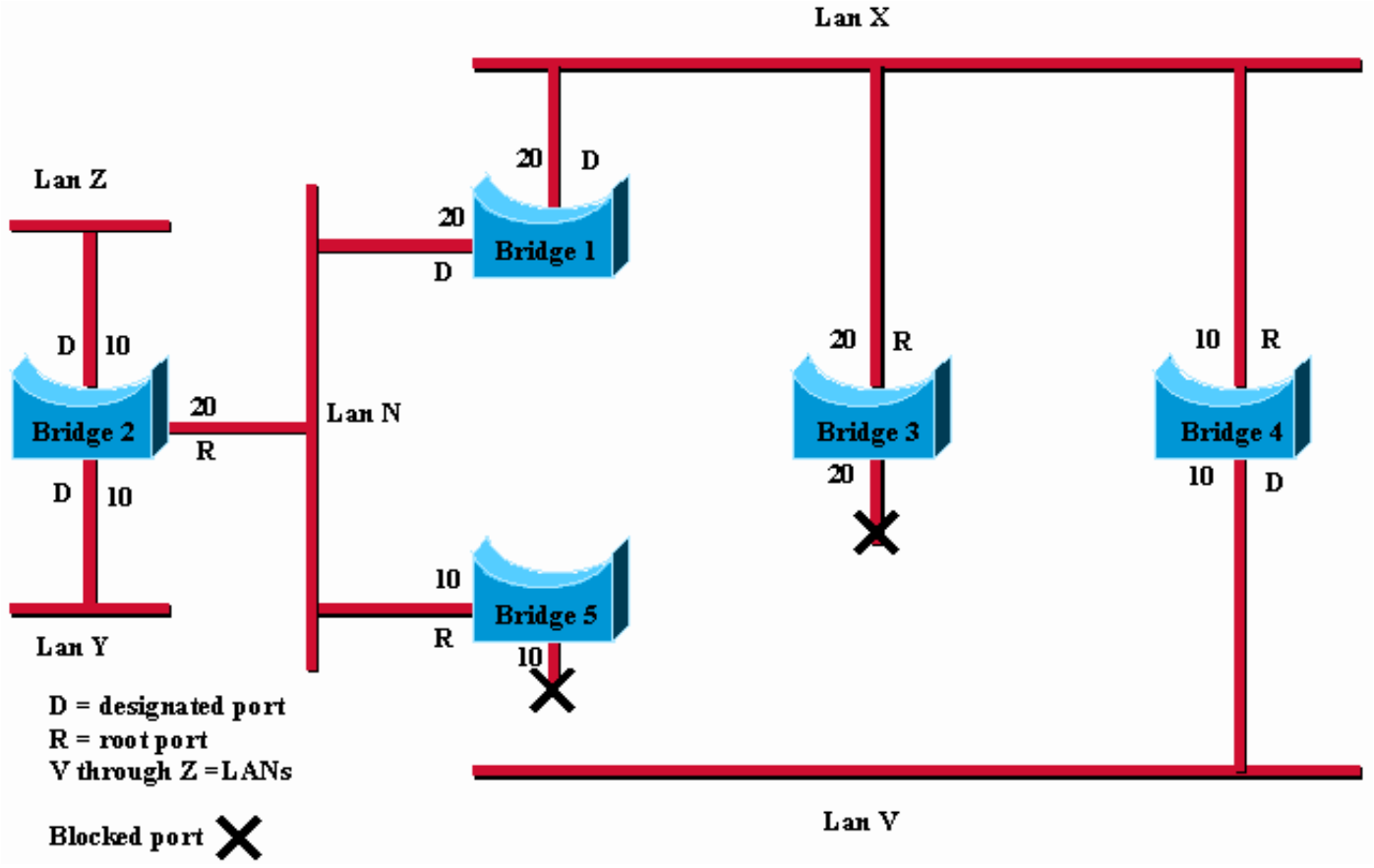


Figura 20-3: Rete bridge trasparente (dopo STA)

Il calcolo dello Spanning Tree viene eseguito quando il bridge è acceso e ogni volta che viene rilevata una modifica della topologia. Il calcolo richiede la comunicazione tra gli Spanning Tree Bridge, che viene eseguita tramite messaggi di configurazione (talvolta denominati BDPU o unità dati di protocollo bridge). I messaggi di configurazione contengono informazioni che identificano il bridge che si presume sia l'identificatore principale (root identifier) e la distanza tra il bridge di invio

e il bridge principale (root path cost). I messaggi di configurazione contengono anche l'identificativo del bridge di invio e la data delle informazioni contenute nel messaggio di configurazione.

I bridge scambiano messaggi di configurazione a intervalli regolari (in genere da uno a quattro secondi). Se un bridge ha esito negativo (con conseguente modifica della topologia), i bridge vicini rilevano presto la mancanza di messaggi di configurazione e avviano un ricalcolo dello Spanning Tree.

Tutte le decisioni trasparenti sulla topologia dei bridge vengono prese localmente. I messaggi di configurazione vengono scambiati tra bridge vicini. Non esiste un'autorità centrale per la topologia o l'amministrazione della rete.

Formato frame

I bridge trasparenti scambiano messaggi di configurazione e messaggi di modifica della topologia. I messaggi di configurazione vengono inviati tra i bridge per stabilire una topologia di rete. I messaggi di modifica della topologia vengono inviati dopo che è stata rilevata una modifica della topologia per indicare che è necessario eseguire di nuovo la STA.

La Tabella 20-2 mostra il formato dei messaggi di configurazione IEEE 802.1d.

Tabella 20-2: Configurazione bridge trasparente

Identificatore protocollo	Versione	Tipo di messaggio	Flag	ID radice	Costo percorso radice	ID bridge	ID porta	Pagina messaggio	Validità massima	Frequenza di invio dei messaggi hello	Ritardo di inoltro
2 byte	1 byte	1 byte	1 byte	8 byte	4 byte	8 byte	2 byte	2 byte	2 byte	2 byte	2 byte

Campi messaggio

I messaggi di configurazione bridge trasparente sono costituiti da 35 byte. Di seguito sono riportati i campi del messaggio:

- Identificatore protocollo: Contiene il valore 0.
- Version: Contiene il valore 0.
- Tipo messaggio: Contiene il valore 0.
- Contrassegno: Un campo di un byte, di cui vengono utilizzati solo i primi due bit. Il bit TC indica una modifica della topologia. Il bit di riconoscimento della modifica della topologia (TCA) è impostato per confermare la ricezione di un messaggio di configurazione con il bit TC impostato.

- ID radice: Identifica il bridge radice e ne elenca la priorità a 2 byte seguita dall'ID a 6 byte.
- Costo percorso radice: Contiene il costo del percorso dal bridge che invia il messaggio di configurazione al bridge radice.
- ID bridge: Identifica la priorità e l'ID del bridge che invia il messaggio.
- ID porta: Identifica la porta da cui è stato inviato il messaggio di configurazione. Questo campo consente di rilevare e gestire i loop creati da più bridge collegati.
- Pagina messaggio: Specifica il tempo trascorso dall'invio del messaggio di configurazione su cui si basa il messaggio di configurazione corrente da parte della radice.
- Durata massima: Indica quando il messaggio di configurazione corrente deve essere eliminato.
- Frequenza di invio dei messaggi hello: Fornisce il periodo di tempo tra i messaggi di configurazione del bridge radice.
- Ritardo di inoltro: Indica il tempo di attesa dei bridge prima di una transizione a un nuovo stato dopo una modifica della topologia. Se un bridge passa troppo presto, non tutti i collegamenti di rete possono essere pronti a modificarne lo stato e possono verificarsi loop.

Il formato del messaggio di modifica della topologia è simile a quello del messaggio di configurazione del bridge trasparente, con la differenza che è composto solo dai primi quattro byte. Di seguito sono riportati i campi del messaggio:

- Identificatore protocollo: Contiene il valore 0.
- Version: Contiene il valore 0.
- Tipo messaggio: Contiene il valore 128.

Diverse tecniche di bridging di IOS

I router Cisco hanno tre modi diversi di implementare il bridging: Funzionamento predefinito, Routing e Bridging simultaneo (CRB) e Routing e Bridging integrato (IRB).

Comportamento predefinito

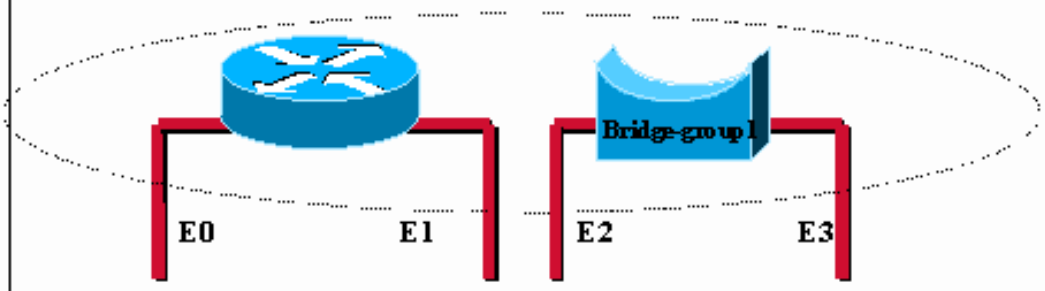
Prima che le funzionalità IRB e CRB fossero disponibili, era possibile eseguire il bridging o il routing di un protocollo solo su base di piattaforma. In altre parole, se è stato usato il comando **ip route**, ad esempio, il routing IP è stato eseguito su tutte le interfacce. In questa situazione, non è possibile collegare l'IP su nessuna delle interfacce del router.

CRB (Concurrent Routing and Bridging)

Con CRB è possibile determinare se eseguire il bridging o il routing di un protocollo su base di interfaccia. In altre parole, è possibile indirizzare un determinato protocollo su alcune interfacce e collegare lo stesso protocollo su interfacce bridge-gruppo all'interno dello stesso router. Il router può quindi essere sia un router sia un bridge per un determinato protocollo, ma non può esistere alcun tipo di comunicazione tra interfacce definite dal routing e interfacce bridge-gruppo.

Nell'esempio viene mostrato che, per un determinato protocollo, un singolo router può logicamente agire come dispositivi separati e indipendenti: un router e uno o più bridge:

```
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).

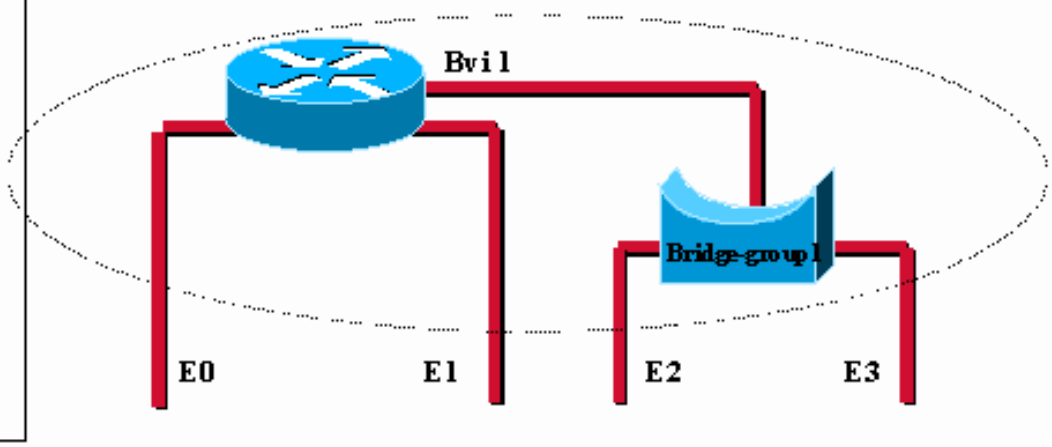
Figura 20-4: CRB (Concurrent Routing and Bridging)

IRB (Integrated Routing and Bridging)

IRB consente di effettuare il routing tra un bridge-group e un'interfaccia di routing tramite un concetto denominato BVI (Bridge-Group Virtual Interface). Poiché il bridging si verifica a livello di collegamento dati e il routing a livello di rete, i modelli di configurazione dei protocolli sono diversi. Con l'IP, ad esempio, le interfacce bridge-group appartengono alla stessa rete e hanno un indirizzo di rete IP collettivo, mentre ogni interfaccia instradata rappresenta una rete distinta con il proprio indirizzo di rete IP.

Il concetto di BVI è stato creato per consentire a queste interfacce di scambiare pacchetti per un dato protocollo. Dal punto di vista concettuale, come mostrato nell'esempio, il router Cisco sembra un router connesso a uno o più gruppi di bridge:

```
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.

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

Il BVI è un'interfaccia virtuale all'interno del router che funziona come una normale interfaccia di routing. Il BVI rappresenta il bridge-group corrispondente alle interfacce instradate all'interno del router. Il numero di interfaccia della BVI è il numero del bridge-group rappresentato da questa interfaccia virtuale. Il numero è il collegamento tra questa BVI e il gruppo-ponte.

Nell'esempio viene mostrato come applicare il principio BVI al Route Switch Module (RSM) di uno switch Catalyst:

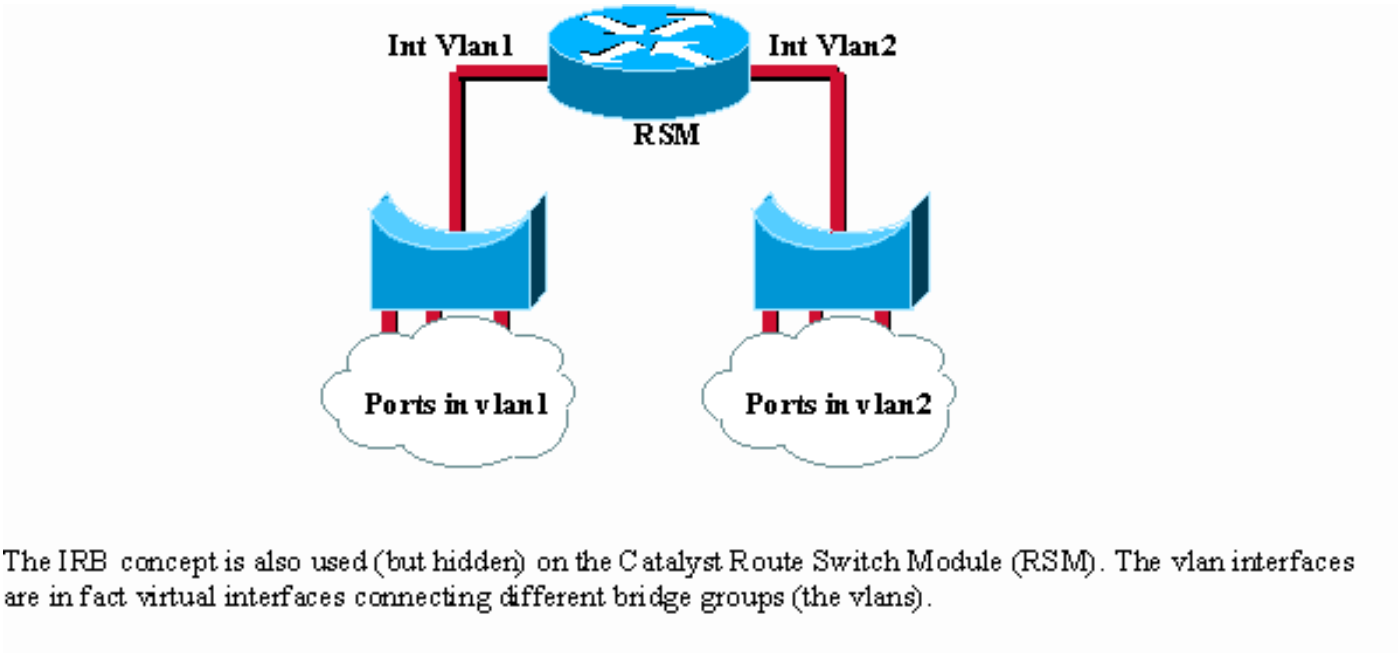


Figura 20-6: Route Switch Module (RSM) in uno switch Catalyst.

Risoluzione dei problemi di Bridging trasparente

In questa sezione vengono presentate informazioni sulla risoluzione dei problemi di connettività nelle interreti con bridging trasparente. Descrive specifici sintomi di bridging trasparenti, i problemi che possono causare ogni sintomo e le soluzioni a tali problemi.

Nota: i problemi associati al bridging origine-route (SRB), al bridging di conversione e al bridging origine-route trasparente (SRT) sono descritti nel Capitolo 10, "Risoluzione dei problemi di IBM".

Per risolvere in modo efficiente i problemi relativi alla rete con bridging, è necessario disporre di una conoscenza di base della progettazione, in particolare quando è coinvolto uno Spanning Tree.

Devono essere disponibili:

- Mappa topologica della rete con bridging
- Posizione del ponte radice
- Posizione del collegamento ridondante (e porte bloccate)

Quando si risolvono i problemi di connettività, ridurre il problema a un numero minimo di host, idealmente solo un client e un server.

In queste sezioni vengono descritti i problemi di rete più comuni nelle reti con bridging trasparente:

- Bridging trasparente: Nessuna connettività

- Bridging trasparente: Spanning Tree instabile
- Bridging trasparente: Sessioni terminate in modo imprevisto
- Bridging trasparente: Tempeste cicliche e broadcast

Bridging trasparente: Nessuna connettività

Sintomo: Il client non può connettersi agli host su una rete con bridging trasparente.

La Tabella 20-3 delinea i problemi che possono causare questo sintomo e suggerisce le soluzioni.

Tabella 20-3: Bridging trasparente: Nessuna connettività

Possibili cause	Azioni consigliate
Problema hardware o multimediale	1. Per verificare la presenza di un problema di connettività, usare il comando **show bridge** EXEC. In questo caso, l'output non visualizzerà alcun indirizzo MAC[1] nella tabella di bridging. 2. Utilizzare il comando show interfaces EXEC per determinare se l'interfaccia e il protocollo di linea sono attivi. 3. Se l'interfaccia non è attiva, risolvere i problemi relativi all'hardware o al supporto. Fare riferimento al capitolo 3, "Risoluzione dei problemi relativi all'hardware e all'avvio". 4. Se il protocollo di linea non è attivo, verificare la connessione fisica tra l'interfaccia e la rete. Verificare che la connessione sia sicura e che i cavi non siano danneggiati. Se il protocollo di linea è attivo ma i contatori dei pacchetti di input e output non sono incrementali, controllare la connettività dei supporti e dell'host. Fare riferimento al capitolo relativo alla risoluzione dei problemi dei supporti relativo al tipo di supporto utilizzato nella rete.
Host inattivo	1. Utilizzare il comando **show bridge** EXEC sui bridge per verificare che la tabella di bridging includa gli indirizzi MAC dei nodi finali collegati. La tabella di bridging comprende gli indirizzi MAC di origine e di destinazione degli host e viene compilata quando i pacchetti di origine o destinazione passano attraverso il bridge. 2. Se mancano nodi finali previsti, controllare lo stato dei nodi per verificare che siano

	connessi e configurati correttamente. 3. Reinizializzare o riconfigurare i nodi finali in base alle esigenze e riesaminare la tabella di bridging con il comando **show bridge**.
Percorso di bridging interrotto	1. Identificare il percorso che i pacchetti devono seguire tra i nodi finali. Se sul percorso è presente un router, suddividere la risoluzione dei problemi in due parti: Nodo 1-Router e Router-Node 2. 2. Connettersi a ciascun bridge sul percorso e controllare lo stato delle porte utilizzate sul percorso tra i nodi finali (come descritto nella voce della tabella "Problemi di hardware o supporti"). 3. Utilizzare il comando **show bridge** per assicurarsi che l'indirizzo MAC dei nodi venga appreso sulle porte corrette. In caso contrario, la topologia dello Spanning Tree potrebbe diventare instabile. Cfr. tabella 20-2, "Bridging trasparente: "Spanning Tree instabile". 4. Verificare lo stato delle porte con il comando **show span**. Se le porte che possono trasmettere il traffico tra i nodi finali non sono nello stato di inoltro, la topologia della struttura può essere cambiata in modo imprevisto. Vedere la Tabella 20-4, "Transparent Bridging Unstable Spanning Tree".
Filtri di bridging non configurati correttamente	1. Per determinare se i filtri bridge sono configurati, usare il comando **show running-config** in modalità di esecuzione privilegiata. 2. Disabilitare i filtri bridge sulle interfacce sospette e determinare se la connettività è ripristinata. 3. Se la connettività non viene ripristinata, il problema non è il filtro. Se la connettività viene ripristinata dopo la rimozione dei filtri, la causa del problema di connettività è uno o più filtri errati. 4. Se esistono più filtri o filtri che utilizzano elenchi di accesso con più istruzioni, applicare ogni filtro singolarmente per identificare il filtro con problemi. Verificare la configurazione per i filtri **LSAP**[2] di input e output e **TYPE**, che possono essere

	utilizzati contemporaneamente per bloccare diversi protocolli. Ad esempio, **LSAP (F0F0)** può essere utilizzato per bloccare NetBIOS e **TYPE (6004)** per bloccare il trasporto locale. 5. Modificare i filtri o gli elenchi degli accessi che bloccano il traffico. Continuare a provare i filtri fino a quando tutti i filtri non sono abilitati e le connessioni funzionano ancora.
Code di input e output piene	Un traffico multicast o broadcast eccessivo può causare l'overflow delle code di input e output, con conseguente perdita dei pacchetti. 1. Usare il comando **show interfaces** per cercare le perdite di input e output. Le cadute suggeriscono un traffico eccessivo sui media. Se il numero corrente di pacchetti nella coda di input è costantemente pari o superiore all'80% delle dimensioni correnti della coda di input, è necessario sintonizzare le dimensioni della coda di input per adattarle alla velocità dei pacchetti. Anche se il numero corrente di pacchetti nella coda di input non sembra mai avvicinarsi alle dimensioni della coda, i burst di pacchetti possono comunque superare la coda. 2. Ridurre il traffico broadcast e multicast sulle reti collegate utilizzando i filtri di bridging o segmentare la rete con più dispositivi internetwork. 3. Se la connessione è un collegamento seriale, aumentare la larghezza di banda, applicare code di priorità, aumentare le dimensioni della coda di attesa o modificare le dimensioni del buffer di sistema. Per ulteriori informazioni, fare riferimento al Capitolo 15, "Risoluzione dei problemi della linea seriale".

[1]MAC = Controllo accesso supporti

[2]LSAP = Access Point dei servizi di collegamento

Bridging trasparente: Spanning Tree instabile

Sintomo: Perdita temporanea di connettività tra gli host. Il problema interessa più host contemporaneamente.

La Tabella 20-4 delinea i problemi che possono causare questo sintomo e suggerisce le soluzioni.

Tabella 20-4: Bridging trasparente: Spanning Tree instabile

Possibili cause	Azioni consigliate
Intermittenza collegamenti	1. Utilizzare il comando **show span** per verificare se il numero di modifiche alla topologia aumenta costantemente. 2. In tal caso, controllare il collegamento tra i bridge con il comando **show interface**. Se il comando non rivela lo sfarfallio del collegamento tra due bridge, usare il comando **debug spantree event** in modalità di esecuzione privilegiata sui bridge. In questo modo vengono registrate tutte le modifiche correlate allo Spanning Tree. In una topologia stabile, non può esserci. Gli unici collegamenti da tracciare sono quelli che collegano tra loro i dispositivi bridge. La transizione su un collegamento a una stazione terminale non dovrebbe avere alcun impatto sulla rete. **Nota:** poiché all'output di debug viene assegnata una priorità alta nel processo CPU, l'utilizzo del comando **debug spantree event** può rendere il sistema inutilizzabile. Per questo motivo, usare i comandi di **debug** solo per risolvere problemi specifici o durante le sessioni per risolvere i problemi con il personale di supporto tecnico Cisco. Inoltre, è meglio usare i comandi di **debug** in periodi di traffico di rete ridotto e meno utenti. Se si esegue il debug entro questi periodi, si riduce la probabilità che un aumento del sovraccarico dei comandi di **debug** influisca sull'utilizzo del sistema.
Il bridge radice continua a cambiare/ più bridge dichiarano di essere il bridge	1. Verificare la coerenza delle informazioni del bridge radice in tutta la rete con bridging tramite i comandi **show span** sui diversi bridge. 2. Se esistono diversi bridge che affermano di essere la radice, accertarsi di eseguire lo stesso protocollo Spanning Tree su ogni bridge (vedere la voce della tabella Spanning Tree algorithm mismatch" nella Tabella 20-6). 3. Utilizzare il comando **bridge** *<gruppo>* **priority** *<numero>* sul bridge radice per forzare il bridge desiderato a diventare la

radice	radice. Più bassa è la priorità, più è probabile che il ponte diventi la radice. 4. Controllare il diametro della rete. Con uno Spanning Tree standard configurato, non devono essere presenti più di sette hop di bridge tra due host.
Hellos non scambiati	1. Verificare se i bridge comunicano tra loro. Utilizzare un analizzatore di rete o il comando **debug spanttree** in modalità di esecuzione privilegiata per verificare se i frame hello dello spanning tree vengono scambiati. **Nota:** poiché all'output di debug viene assegnata una priorità alta nel processo CPU, l'utilizzo del comando **debug spantree event** può rendere il sistema inutilizzabile. Per questo motivo, usare i comandi di **debug** solo per risolvere problemi specifici o durante le sessioni per risolvere i problemi con il personale di supporto tecnico Cisco. Inoltre, è meglio usare i comandi di **debug** in periodi di traffico di rete ridotto e meno utenti. Se si esegue il debug entro questi periodi, si riduce la probabilità che un aumento del sovraccarico dei comandi di **debug** influisca sull'utilizzo del sistema. 2. Se gli helper non vengono scambiati, controllare le connessioni fisiche e la configurazione software sui bridge.

Bridging trasparente: Sessioni terminate in modo imprevisto

Sintomo: Le connessioni in un ambiente con bridging trasparente sono state stabilite correttamente, ma a volte le sessioni terminano improvvisamente.

La Tabella 20-5 delinea i problemi che possono causare questo sintomo e suggerisce le soluzioni.

Tabella 20-5: Bridging trasparente: Sessioni terminate in modo imprevisto

Possibili cause	Azioni consigliate
Ritrasmissioni eccessive	1. Utilizzare un analizzatore di rete per cercare ritrasmissioni host. 2. Se le ritrasmissioni vengono visualizzate su linee seriali lente, aumentare i timer di trasmissione sull'host. Per informazioni su come configurare gli host, consultare la

	documentazione del fornitore. Per informazioni su come risolvere i problemi relativi alle linee seriali, fare riferimento al Capitolo 15, "Risoluzione dei problemi relativi alle linee seriali". Se vengono visualizzate ritrasmissioni su supporti LAN ad alta velocità, verificare la presenza di pacchetti inviati e ricevuti in ordine o scartati da dispositivi intermedi (ad esempio un bridge o uno switch). Risolvere i problemi relativi al supporto LAN. Per ulteriori informazioni, consultare il capitolo relativo alla risoluzione dei problemi relativi ai supporti utilizzati nella rete. 3. Utilizzare un analizzatore di rete per determinare se il numero di ritrasmissioni è minore.
Ritardo eccessivo sul collegamento seriale	Aumentare la larghezza di banda, applicare l'accodamento priorità, aumentare le dimensioni della coda di attesa o modificare le dimensioni del buffer di sistema. Per ulteriori informazioni, fare riferimento al Capitolo 15, "Risoluzione dei problemi della linea seriale".

Bridging trasparente: Tempeste cicliche e broadcast

Sintomo: Le tempeste di trasmissione e loop di pacchetti si verificano in ambienti bridge trasparenti. Le stazioni terminali sono costrette a ritrasmettere in modo eccessivo, il che provoca il timeout o la caduta delle sessioni.

Nota: i loop di pacchetto sono in genere causati da problemi di progettazione della rete o da problemi hardware.

La Tabella 20-6 delinea i problemi che possono causare questo sintomo e suggerisce le soluzioni.

I loop di bridging rappresentano lo scenario peggiore in una rete con bridging in quanto potrebbero influire su tutti gli utenti. In caso di emergenza, il modo migliore per ripristinare rapidamente la connettività è disabilitare manualmente tutte le interfacce che forniscono percorsi ridondanti nella rete. Sfortunatamente, la causa del ciclo di bridging sarà molto difficile da identificare in seguito. Se possibile, provare prima le azioni della Tabella 20-6.

Tabella 20-6: Bridging trasparente: Tempeste cicliche e broadcast

Possibili cause	Azioni consigliate
Spanning Tree non	1. Esaminare una mappa della topologia della rete interna per verificare la

implementato	presenza di eventuali loop. 2. Eliminare eventuali loop esistenti o verificare che i collegamenti appropriati siano in modalità di backup. 3. Se i temporali e i loop di pacchetto persistono, usare il comando **show interfaces** EXEC per ottenere le statistiche sul numero di pacchetti di input e output. Se questi contatori aumentano a una velocità insolitamente elevata (rispetto ai normali carichi di traffico), è probabile che nella rete sia ancora presente un loop. 4. Implementare un algoritmo Spanning Tree per impedire la formazione di loop.
Mancata corrispondenza dell'algoritmo Spanning Tree	1. Usare il comando **show span** EXEC su ciascun bridge per determinare l'algoritmo dello spanning tree da usare. 2. Verificare che tutti i bridge eseguano lo stesso algoritmo Spanning Tree (DEC o IEEE)[1]. Può essere necessario utilizzare sia l'algoritmo DEC che l'algoritmo IEEE Spanning Tree nella rete per alcune configurazioni molto specifiche (generalmente, quelle che coinvolgono l'IRB). Se la mancata corrispondenza nel protocollo Spanning Tree non è prevista, riconfigurare i bridge in modo che tutti i bridge utilizzino lo stesso algoritmo Spanning Tree. **Nota:** gli algoritmi Spanning Tree DEC e IEEE sono incompatibili.
Configurazione errata di più domini di bridging	1. Utilizzare il comando **show span** EXEC sui bridge per verificare che tutti i numeri dei gruppi di dominio corrispondano ai domini di bridging specificati. 2. Se per il bridge sono configurati più gruppi di dominio, verificare che tutte le specifiche di dominio siano assegnate correttamente. Utilizzare il comando di configurazione globale **bridge** <*group*> **domain** <domain-number> per apportare le modifiche

	necessarie. 3. Verificare che non esistano loop tra i domini di bridging. Un ambiente di bridging tra domini non fornisce la prevenzione dei loop basata sullo spanning tree. Ogni dominio ha il proprio spanning tree, che è indipendente dallo spanning tree negli altri domini.
Errore di collegamento (collegamento unidirezionale), mancata corrispondenza del duplex, livello elevato di errore su una porta.	I loop si verificano quando una porta che deve bloccare passa allo stato di inoltro. Una porta deve ricevere i BPDU da un bridge vicino per poter rimanere nello stato di blocco. Qualsiasi errore che provochi la perdita di BPDU può quindi essere la causa di un loop di bridging. 1. Identificare le porte bloccanti dal diagramma di rete. 2. Verificare lo stato delle porte che devono essere bloccate nella rete con bridging con i comandi **show interface** e **show bridge** EXEC. 3. Se si trova una porta probabilmente bloccata che sta inoltrando o sta per inoltrare (ossia, nello stato di apprendimento o ascolto), è stata individuata la vera origine del problema. Verificare se la porta riceve BPDU. In caso contrario, è probabile che si sia verificato un problema sul collegamento connesso a questa porta. controllare quindi gli errori di collegamento, le impostazioni duplex e così via). Se la porta continua a ricevere BPDU, passare al bridge che si prevede verrà designato per questa LAN. Controllare quindi tutti i collegamenti del percorso verso la radice. È possibile riscontrare un problema in uno di questi collegamenti, a condizione che il diagramma di rete iniziale sia corretto.

[1]IEEE = Istituto dei tecnici elettrici ed elettronici

Prima di chiamare il team TAC di Cisco Systems

Quando la rete è stabile, raccogliere quante più informazioni possibile sulla relativa topologia.

Raccogli almeno questi dati:

- Topologia fisica della rete
- Percorso previsto del bridge radice (e del bridge radice di backup)
- Posizione delle porte bloccate

Origini aggiuntive

Libri:

- Interconnessioni, ponti e router, Radia Perlman, Addison-Wesley
- Cisco Lan Switching, K.Clark, K.Hamilton, Cisco Press

Informazioni correlate

- Documentazione sul bridging trasparente
- Documentazione e supporto tecnico – Cisco Systems