# Comprendere i miglioramenti della funzionalità Spanning Tree PortFast BPDU Guard

## Sommario



## Introduzione

Questo documento descrive le funzionalità di miglioramento della protezione BPDU (PortFast Bridge Protocol Data Unit) dello Spanning Tree Protocol (STP).

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Queste versioni software hanno introdotto la protezione BPDU STP PortFast:

- Software Catalyst OS (CatOS) versione 5.4.1 per le piattaforme Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G e 2980G

- Software Cisco IOS® versione 12.0(7)XE per le piattaforme Catalyst 6500/6000
- Software Cisco IOS release 12.1(8a)EW per Catalyst 4500/4000 Supervisor Engine III
- Software Cisco IOS release 12.1(12c)EW per Catalyst 4500/4000 Supervisor Engine IV
- Software Cisco IOS release 12.0(5)WC5 per Catalyst serie 2900XL e 3500XL
- Software Cisco IOS release 12.1(11)AX per gli switch Catalyst serie 3750
- Software Cisco IOS release 12.1(14)AX per switch Catalyst 3750 Metro
- Software Cisco IOS release 12.1(19)EA1 per gli switch Catalyst serie 3560
- Software Cisco IOS release 12.1(4)EA1 per gli switch Catalyst serie 3550
- Software Cisco IOS release 12.1(11)AX per gli switch Catalyst serie 2970
- Software Cisco IOS release 12.1(12c)EA1 per gli switch Catalyst serie 2955
- Software Cisco IOS release 12.1(6)EA2 per gli switch Catalyst serie 2950
- Software Cisco IOS release 12.1(11)EA1 per switch Catalyst 2950 Long-Reach Ethernet (LRE)
- Software Cisco IOS release 12.1(13)AY per gli switch Catalyst serie 2940

---

 Nota: la funzione di protezione BPDU STP PortFast non è disponibile sugli switch Catalyst serie 8500, 2948G-L3 o 4908G-L3.

---

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

## Premesse

Questo documento spiega la funzione di protezione BPDU (PortFast Bridge Protocol Data Unit). Questa funzionalità è una delle migliorie apportate allo Spanning Tree Protocol (STP) da Cisco. Questa funzione migliora l'affidabilità, la gestibilità e la sicurezza della rete degli switch.

## Descrizione delle funzionalità

L'STP configura la topologia mesh in una topologia ad albero priva di loop. Quando il collegamento su una porta bridge diventa attivo, su tale porta viene eseguito il calcolo STP. Il risultato del calcolo è la transizione della porta allo stato di inoltro o di blocco. Il risultato dipende dalla posizione della porta nella rete e dai parametri STP. Questo calcolo e il periodo di transizione richiedono in genere da 30 a 50 secondi. In quel momento, i dati dell'utente non passano attraverso la porta. Alcune applicazioni utente possono scadere durante il periodo.

Per consentire la transizione immediata della porta allo stato di inoltro, abilitare la funzione STP PortFast. PortFast fa passare immediatamente la porta alla modalità di inoltro STP dopo il collegamento. La porta partecipa ancora all'STP. Pertanto, se la porta deve far parte del loop, alla fine passa alla modalità di blocco STP.

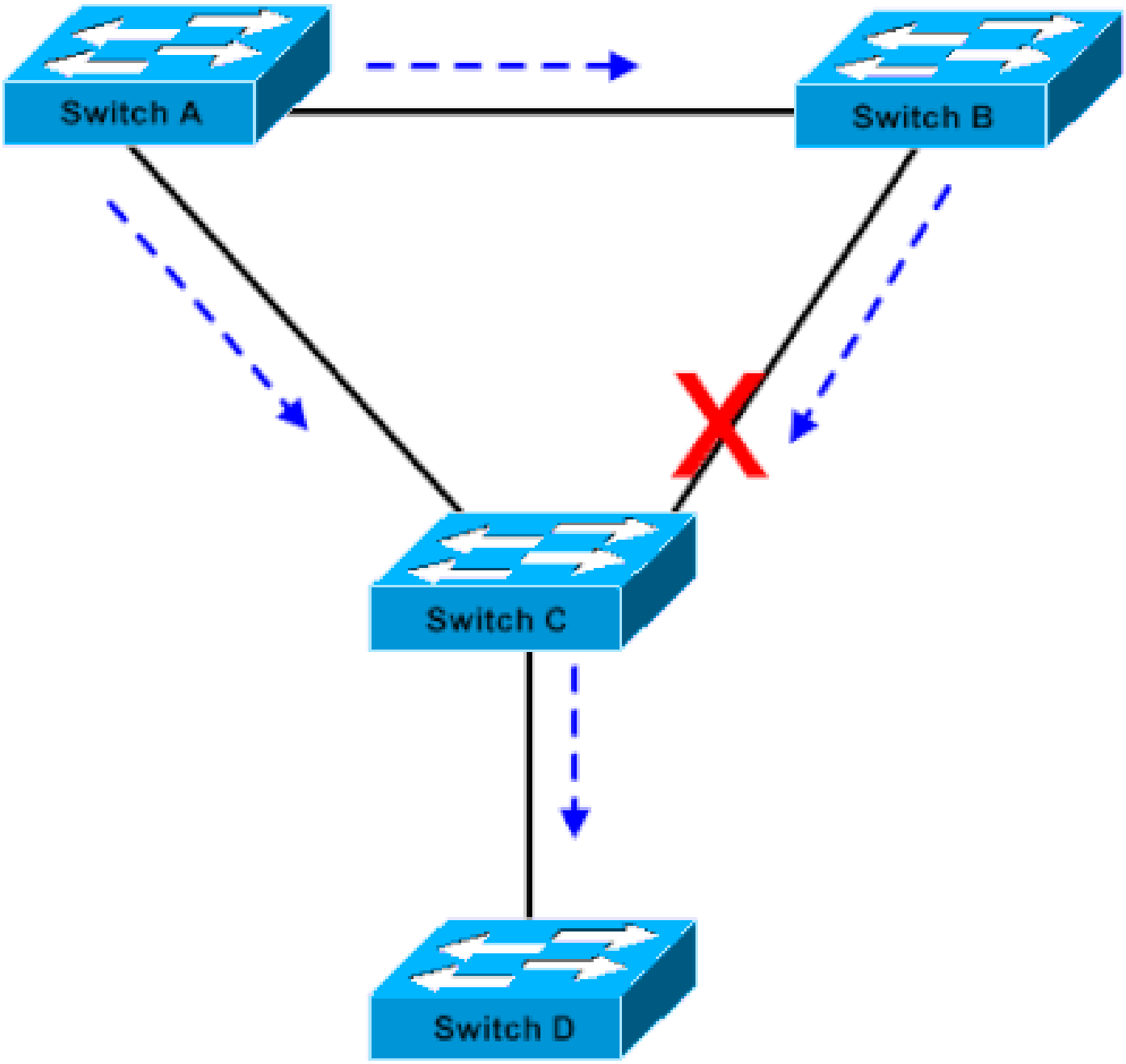
Finché la porta partecipa a STP, alcuni dispositivi possono assumere la funzione di bridge radice e influire sulla topologia STP attiva. Per assumere la funzione di ponte principale, il dispositivo sarebbe collegato alla porta ed eseguirebbe STP con una priorità di ponte inferiore a quella del ponte principale corrente. Se un altro dispositivo assume la funzione di ponte principale in questo modo, la rete viene resa non ottimale. Si tratta di una semplice forma di attacco DoS (Denial of Service) alla rete. L'introduzione temporanea e la successiva rimozione di dispositivi STP con bassa priorità (0) del bridge causano un ricalcolo permanente di STP.

Il miglioramento della funzionalità BPDU Guard di STP PortFast consente ai progettisti di rete di applicare i bordi del dominio STP e di mantenere prevedibile la topologia attiva. I dispositivi dietro le porte con STP PortFast abilitata non sono in grado di influenzare la topologia STP. Alla ricezione di BPDU, l'operazione BPDU Guard disabilita la porta con PortFast configurata. BPDU Guard porta la porta in stato err-disabled e viene visualizzato un messaggio sulla console. Questo messaggio è un esempio:

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

Considerate questo esempio:

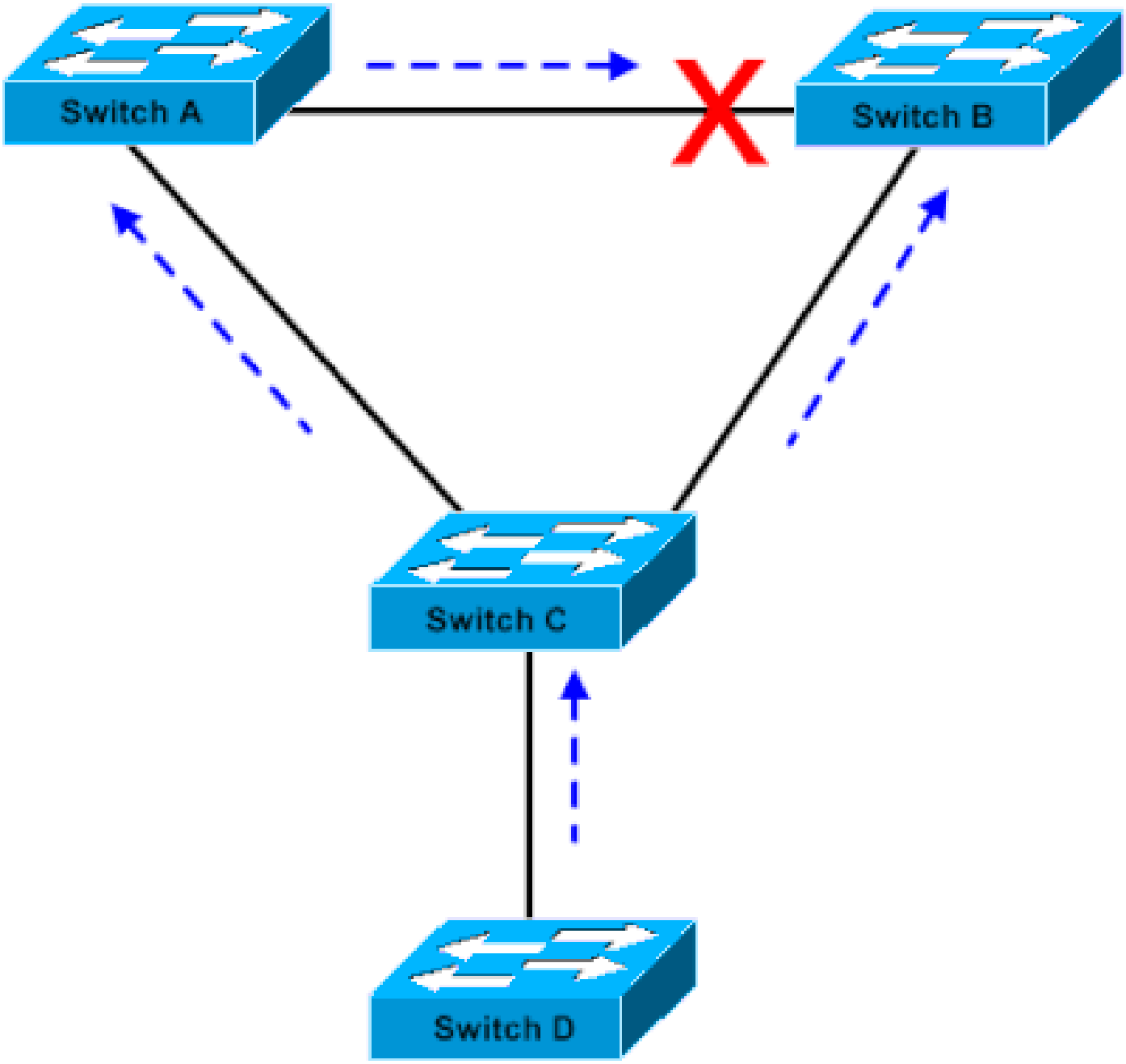
Figura 1




Connessione bridge

Il bridge A ha priorità 8192 e rappresenta la radice della VLAN. Il bridge B ha priorità 16384 ed è il bridge radice di backup per la stessa VLAN. I ponti A e B, connessi tramite un collegamento Gigabit Ethernet, costituiscono un nucleo della rete. Il bridge C è uno switch di accesso e dispone di PortFast configurata sulla porta che si connette al dispositivo D. Se gli altri parametri STP sono predefiniti, la porta C del bridge che si connette al bridge B è in stato di blocco STP. Il dispositivo D (PC) non partecipa al protocollo STP. Le frecce tratteggiate indicano il flusso delle BPDU STP.

Figura 2




L'applicazione Bridge basata su Linux viene avviata su un PC

Nella Figura 2, il dispositivo D ha iniziato a partecipare all'STP. Ad esempio, un'applicazione bridge basata su Linux viene avviata su un PC. Se la priorità del bridge software è 0 o qualsiasi valore inferiore alla priorità del bridge radice, il bridge software assume la funzione di bridge radice. Il collegamento Gigabit Ethernet che connette i due switch core passa alla modalità di blocco. In seguito alla transizione, tutti i dati della VLAN passano attraverso il collegamento a 100 Mbps. Se il flusso di dati attraverso il core della VLAN è superiore a quello che il collegamento può supportare, si verifica la perdita di frame. La perdita di frame determina un'interruzione della connettività.

La funzione di protezione BPDU STP PortFast previene una situazione di questo tipo. Questa funzione disabilita la porta non appena il bridge C riceve la BPDU STP dal dispositivo D.

# Configurazione

È possibile abilitare o disabilitare BPDU Guard PortFast STP su base globale, il che influisce su tutte le porte su cui è configurata PortFast. Per impostazione predefinita, STP BPDU Guard è disabilitato. Per abilitare la protezione BPDU PortFast STP sullo switch, eseguire questo comando:

Comando CatOS

<#root>

```
Console> (enable)
set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.
Console> (enable)
```

Comando software Cisco IOS®

<#root>

```
CatSwitch-IOS(config)#
spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

Quando la funzione STP BPDU Guard disabilita la porta, questa rimane in stato disabled a meno che la porta non venga abilitata manualmente. È possibile configurare una porta in modo che venga riattivata automaticamente dallo stato err-disabled. Utilizzare questi comandi, per impostare l'intervallo di timeout di errdisable e abilitare la funzione di timeout:

Comandi CatOS

<#root>

```
Console> (enable)
set errdisable-timeout interval 400

Console> (enable)
set errdisable-timeout enable bpdu-guard
```

Comandi Cisco IOS Software

<#root>

```
CatSwitch-IOS(config)#
errdisable recovery cause bpduguard

CatSwitch-IOS(config)#
errdisable recovery interval 400
```

Nota: l'intervallo di timeout predefinito è 300 secondi; per impostazione predefinita, la funzione di timeout è disabilitata.

# Monitor (Monitora)

Per verificare se la funzione è abilitata o disabilitata, usare il comando successivo.

## Output comando

Comando CatOS

<#root>

```
Console> (enable)
show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.

Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

   1         0         0        0          1          1

   3         0         0        0          1          1

   4         0         0        0          1          1

  20         0         0        0          1          1
```

```
Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

Total        0         0        0          4          4

Console> (enable)
```

### Comando software Cisco IOS

### <#root>

```
CatSwitch-IOS#

show spanning-tree summary totals

Root bridge for: none.

PortFast BPDU Guard is enabled

UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short


Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                  0         0         0          1          1

CatSwitch-IOS#
```

## Informazioni correlate

- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).