

Migliorare il protocollo STP (Spanning Tree Protocol) con Root Guard

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Descrizione delle funzionalità](#)

[Disponibilità](#)

[Configurazione](#)

[Configurazione nel software Cisco IOS per Catalyst 6500/6000 e Catalyst 4500/4000](#)

[Configurazione nel software Cisco IOS per Catalyst 2900XL/3500XL, 2950 e 3550](#)

[Qual è la differenza tra BPDU Guard e Root Guard nel protocollo STP](#)

[Root Guard consente di risolvere il problema dei due root](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive le migliorate funzioni di protezione root STP che migliorano l'affidabilità, la gestibilità e la sicurezza della rete commutata.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Descrizione delle funzionalità

Il protocollo STP standard non fornisce alcun mezzo per consentire all'amministratore di rete di applicare in modo sicuro la topologia della rete commutata di livello 2 (L2). Un mezzo per applicare la topologia può essere particolarmente importante nelle reti con controllo amministrativo condiviso, in cui diverse entità amministrative o aziende controllano un'unica rete commutata.

Viene calcolata la topologia di inoltro della rete commutata. Il calcolo si basa sulla posizione del root bridge, oltre ad altri parametri. Qualsiasi switch può essere il root bridge in una rete, ma una topologia di inoltro ottimale colloca il root bridge in una posizione predeterminata specifica. Con il protocollo STP standard, qualsiasi bridge nella rete con un ID bridge di livello inferiore assume il ruolo di root bridge. L'amministratore non può applicare la posizione del root bridge.

 Nota: l'amministratore può impostare la priorità del root bridge su 0 per assicurarne la posizione, ma non c'è alcuna garanzia riguardo a un bridge con una priorità pari a 0 e un MAC address di livello inferiore.

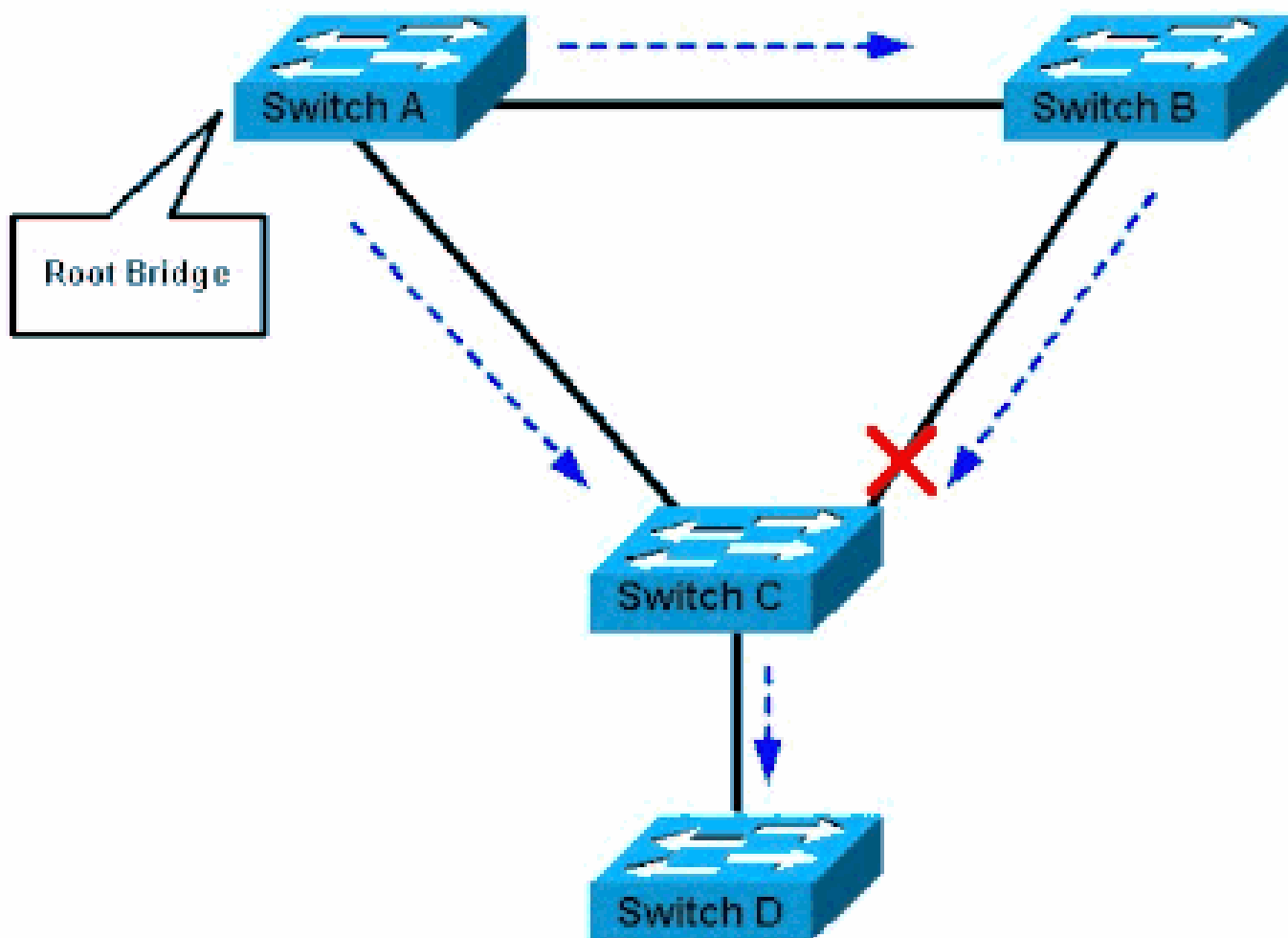
La funzionalità Root Guard offre un modo per applicare la posizione del root bridge nella rete.

Questa opzione garantisce inoltre che tale funzionalità venga attivata sulla porta designata. In genere, tutte le porte del root bridge sono porte designate, a meno che due o più porte del root bridge non siano collegate tra loro. Se il bridge riceve un numero maggiore di BPDU (Bridge Protocol Data Units) del protocollo STP su una porta abilitata per Root Guard, quest'ultima imposta la porta su uno stato STP di incoerenza root. Lo stato di incoerenza root è l'equivalente dello stato di ascolto. Su questa porta il traffico non viene reindirizzato, così Root Guard applica la posizione del root bridge.

L'esempio in questa sezione mostra come un root bridge non autorizzato può causare problemi sulla rete e come la funzionalità Root Guard può essere utile.

Nell'immagine 1, gli switch A e B costituiscono il nucleo della rete e A è il bridge radice per una VLAN. Lo switch C è uno switch di livello di accesso. Il collegamento tra B e C è bloccato sul lato C. Le frecce indicano il flusso di BPDU del protocollo STP.

Immagine 1



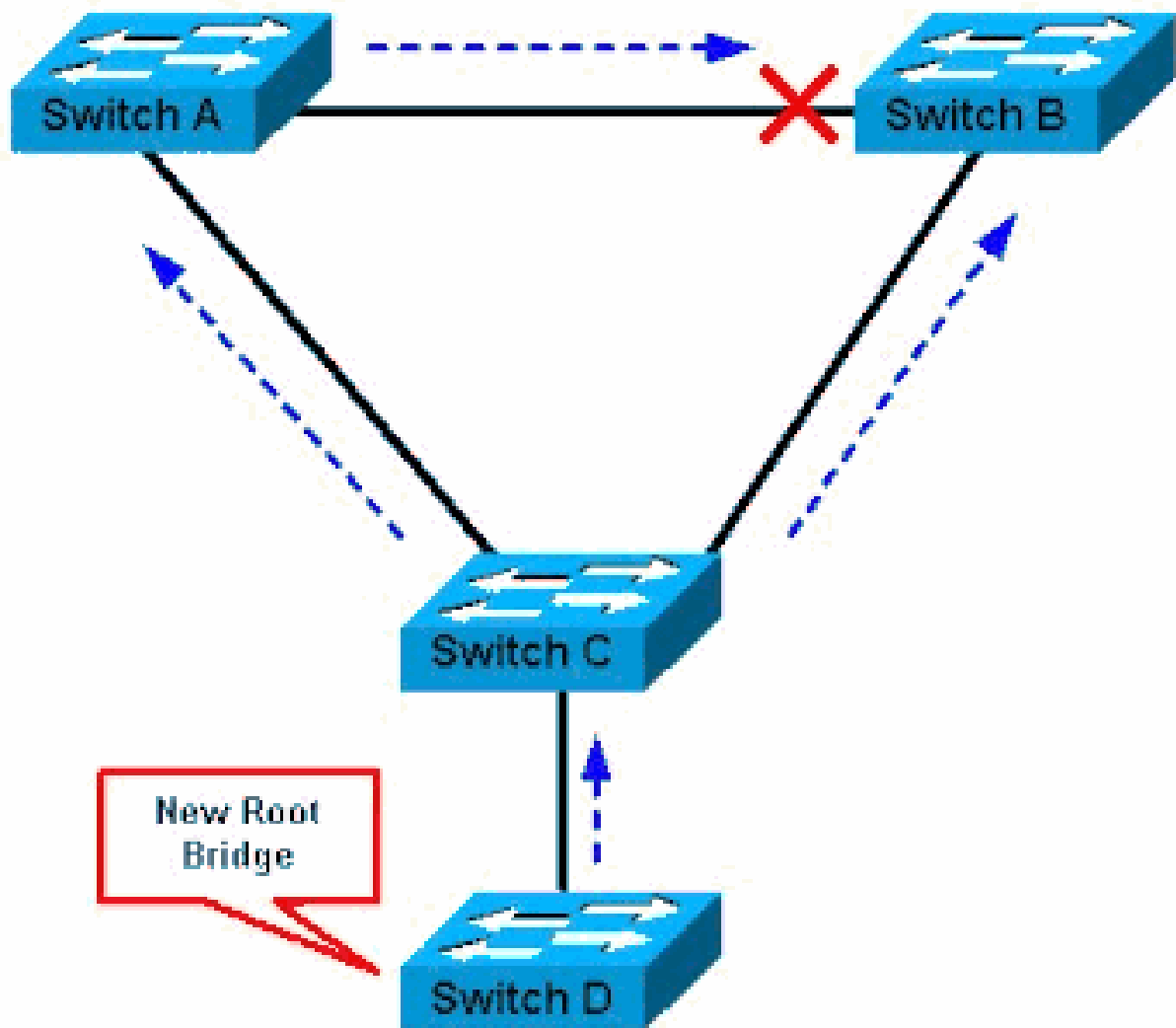
Lo switch A è il bridge radice

Nell'immagine 2, il dispositivo D inizia a partecipare a STP. Ad esempio, le applicazioni bridge basate su software vengono avviate sui PC o su altri switch connessi a una rete di provider di servizi. Se la priorità del bridge D è 0 o qualsiasi valore inferiore alla priorità del root bridge, il dispositivo D viene eletto come root bridge per questa VLAN. Se il collegamento tra i dispositivi A e B è di 1 gigabit e i collegamenti tra A e C e tra B e C sono di 100 Mbps, l'individuazione di D come root causa il blocco del collegamento Gigabit Ethernet tra i due switch principali.

Questo blocco provoca il flusso di tutti i dati nella VLAN in questione tramite un collegamento a 100 Mbps attraverso il livello di accesso. Se la VLAN contiene più dati rispetto a quelli che questo collegamento è in grado di gestire tramite il core, si verifica la perdita di alcuni frame.

L'eliminazione dei frame comporterà una perdita di prestazioni o un'interruzione della connettività.

Immagine 2



Lo switch D è un nuovo bridge radice

La funzionalità Root Guard protegge la rete da questi problemi.

La configurazione di Root Guard è effettuata in base alla porta. La funzionalità Root Guard non consente alla porta di diventare una porta root STP, pertanto la porta è sempre designata come STP. Se una BPDU migliore arriva su questa porta, Root Guard non prende in considerazione la BPDU e sceglie un nuovo root STP. Al contrario, Root Guard mette la porta nello stato STP di incoerenza root. È necessario abilitare root guard su tutte le porte in cui il bridge radice non deve essere visualizzato. In un certo senso, è possibile configurare un perimetro intorno alla parte della rete in cui è possibile posizionare il root STP.

[InImage 2](#), abilitare la protezione root sulla porta dello switch C che si connette allo switch D.

Lo switch C [inImage 2](#) blocca la porta che si connette allo switch D, dopo che lo switch riceve una BPDU superiore. Root Guard mette la porta nello stato STP di incoerenza root. Attraverso la porta in questo stato non passa traffico. Dopo che il dispositivo D ha smesso di inviare BPDU superiori, la porta viene sbloccata di nuovo. Tramite STP, la porta passa dallo stato di ascolto allo stato di apprendimento e alla fine allo stato di inoltro. Il recupero è automatico; non è necessario alcun

intervento umano.

Questo messaggio viene visualizzato dopo che Root Guard ha bloccato una porta:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.  
Moved to root-inconsistent state
```

Disponibilità

Root Guard è disponibile negli switch Catalyst 6500/6000 con software di sistema Cisco IOS®. Questa funzione è stata introdotta per la prima volta nel software Cisco IOS versione 12.0(7)XE. Per Catalyst 4500/4000 che esegue il software di sistema Cisco IOS, questa funzionalità è disponibile in tutte le versioni.

Per gli switch Catalyst 2900XL e 3500XL, la funzionalità Root Guard è disponibile nella versione del software Cisco IOS 12.0(5)XU e in versioni successive. Gli switch Catalyst serie 2950 supportano la funzionalità Root Guard nella versione del software Cisco IOS 12.0(5.2)WC(1) e in versioni successive. Gli switch Catalyst serie 3550 supportano la funzionalità Root Guard nella versione del software Cisco IOS 12.1(4)EA1 e in versioni successive.

Questa funzione è disponibile anche sui nuovi switch Cisco Catalyst serie 1000.

Configurazione

Configurazione nel software Cisco IOS per Catalyst 6500/6000 e Catalyst 4500/4000

Negli switch Catalyst 6500/6000 o Catalyst 4500/4000 che eseguono il software di sistema Cisco IOS, eseguire questa serie di comandi per configurare Root Guard per il protocollo STP:

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
!
```


```
Switch#(config)#
```

```
interface fastethernet 3/1
```

```
Switch#(config-if)#
```

```
spanning-tree guard root
```

```
!
```

 Nota: nella versione del software Cisco IOS 12.1(3a)E3 per Catalyst 6500/6000 che esegue il software di sistema Cisco IOS, questo comando è stato modificato da spanning-tree rootguard a spanning-tree guard root. Il Catalyst 4500/4000 che esegue il software di sistema Cisco IOS utilizza il comando spanning-tree guard root in tutte le versioni.

Configurazione nel software Cisco IOS per Catalyst 2900XL/3500XL, 2950 e 3550

Su Catalyst 2900XL, 3500XL, 2950 e 3550, configurare gli switch con Root Guard in modalità di configurazione interfaccia, come mostrato nell'esempio seguente:

```
<#root>
```

```
Switch#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#
```

```
interface fastethernet 0/8
```

```
Switch(config-if)#
```

```
spanning-tree rootguard
```

```
Switch(config-if)#
```

```
^Z
```

```
*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on  
port FastEthernet0/8 VLAN 1.
```

```
Switch#
```

Qual è la differenza tra BPDU Guard e Root Guard nel protocollo STP

BPDU Guard e Root Guard sono simili, ma il loro impatto è diverso. BPDU Guard disabilita la porta alla ricezione di BPDU se PortFast è abilitato sulla porta. La disabilitazione impedisce effettivamente ai dispositivi dietro tali porte di partecipare a STP. È necessario riattivare manualmente la porta messa in stato errdisable o configurare errdisable-timeout.

La funzionalità Root Guard consente al dispositivo di partecipare a STP a condizione che il dispositivo non tenti di diventare il root. Se Root Guard blocca la porta, il ripristino successivo è automatico. Il ripristino si verifica quando il dispositivo non invia più BPDU di qualità superiore.

Per ulteriori informazioni su BPDU Guard, vedere [Miglioramenti della funzionalità Spanning Tree PortFast BPDU Guard](#).

Root Guard consente di risolvere il problema dei due root

Può verificarsi un errore di collegamento unidirezionale tra due bridge in una rete. A causa dell'errore, un bridge non riceve le BPDU dal root bridge. In questo caso, lo switch root riceve i frame inviati da altri switch, ma gli altri switch non ricevono le BPDU inviate dallo switch root. Questo può portare a un loop STP. Poiché gli altri switch non ricevono alcuna BPDU dal root, credono di essere il root e iniziano a inviare le BPDU.

Quando il root bridge effettivo inizia a ricevere le BPDU, il root le ignora perché non sono di livello superiore. Il root bridge non cambia. Pertanto, Root Guard non contribuisce alla risoluzione di questo problema. Le funzionalità UniDirectional Link Detection (UDLD) e Loop Guard consentono di risolvere questo problema.

Per ulteriori informazioni sugli scenari di errore STP e su come risolverli, vedere [Spanning Tree Protocol Problems and Related Design Considerations](#) (Problemi del protocollo Spanning Tree e considerazioni correlate sulla progettazione).

Informazioni correlate

- [Descrizione e configurazione della funzionalità del protocollo UDLD](#)
- [Ripristino di una porta disabilitata a causa di un errore sulle piattaforme Cisco IOS](#)
- [Supporto tecnico Cisco e download](#)

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).