

Procedure ottimali per la migrazione di più Spanning Tree

Obiettivo

L'obiettivo di questo documento è quello di fornire procedure ottimali per la migrazione a Multiple Spanning Tree (MSTP). L'utilizzo di MSTP su altre varianti dello Spanning Tree può migliorare l'efficienza e l'affidabilità della rete.

Requisiti

- La necessità di ottimizzare il layer 2 in un ambiente hardware misto
 - Switch Cisco per piccole imprese
 - Serie Sx250 ([Guida All'Amministrazione](#))
 - Serie Sx300 ([Guida All'Amministrazione](#))
 - Serie Sx350 ([Guida All'Amministrazione](#))
 - Serie SG350X ([Guida all'amministrazione](#))
 - Serie Sx550X ([Guida All'Amministrazione](#))
 - Switch Cisco Catalyst
- Conoscenza pratica dello Spanning Tree ([ulteriori informazioni](#))
- Wireshark (facoltativo)

Sommario

1. [Terminologia MSTP](#)
2. [Best Practice #1 - Verifica della necessità di eseguire la migrazione a MSTP](#)
3. [Best Practice 2: strategia della migrazione](#)
4. [Best Practice #3 - Best Practice #3 - Abilitazione delle porte point-to-point all'utilizzo di PortFast](#)
5. [Best Practice n. 4 - Abilitazione di BPDU Guard sulle porte edge](#)
6. [Best Practice 5: mappatura delle VLAN agli MSTI, non all'IST \(MST0\)](#)
7. [Best Practice n. 6: collocazione di tutti gli switch abilitati per MSTP nella stessa area](#)
8. [Best Practice n. 7 - Nidificare il bridge radice del CIST nell'area MST principale](#)
9. [Verifica della migrazione - È attiva questa opzione?](#)
10. [Conclusioni](#)

Struttura della guida

In questa guida non verranno descritti i passaggi come accedere al dispositivo tramite SSH o l'interfaccia di gestione, ma verranno evidenziati i comandi principali. Ciascuna procedura ottimale contiene una sottoattività in cui vengono delineati i passaggi appropriati per l'hardware Cisco misto (Enterprise e SMB). Per le guide alla configurazione, vedere i due collegamenti seguenti:

- [Configurazione di MSTP sullo switch SMB](#)
- [Configurazione di MSTP su switch Catalyst](#)

Terminologia MSTP

Questa sezione ha lo scopo di fornire un modello mentale accessibile del protocollo in gioco. Le definizioni sono componenti di interblocco del protocollo MSTP. Ulteriori dettagli sono contenuti nei punti secondari.

BPDU - Bridge Protocol Data Unit: si tratta di frame multicast contenenti tutte le informazioni necessarie a uno switch per continuare a funzionare.

Nota: verificare che i mapping di istanza non siano presenti nella BPDU.

Regione - (*specifica di MSTP*) - Una regione risolve il problema incontrato da altri gusti di STP che inviano un BPDU per VLAN. Come con lo Spanning Tree per Vlan, l'invio di un numero così elevato di BPDU provoca un sovraccarico della CPU e quindi riduce le prestazioni della rete. Al contrario, con il protocollo MSTP tutte le VLAN sono mappate su un'unica area.

Istanza: un'istanza è un insieme di tabelle logiche di una VLAN, o di molte VLAN, relative a una determinata area. Questa istanza viene quindi mappata a una zona. Questi passaggi verranno completati come parte della migrazione.

L'istanza predefinita 0 (zero) è sinonimo dei seguenti termini *MST0*, *Internal Spanning Tree (IST)*.

Le istanze create dall'utente vengono definite istanze Multiple Spanning Tree o MSTI.

In questo modo, una buona documentazione delle VLAN della rete consente di evitare i problemi.

- Se un'istanza non riesce, non influirà su altre istanze.

MSTI - Più istanze Spanning Tree - Contiene l'istanza creata dall'amministratore. Queste mappature sono contenute in ciò che è noto come "MRecord", visibile tramite Wireshark. I record contengono i dettagli necessari per gestire la topologia dell'istanza.

IST - Internal Spanning Tree - è il record degli switch che partecipano a una zona MSTP. Gli switch (indipendentemente dal numero) contenuti in una zona vengono rappresentati nelle aree esterne come un unico switch.

- **CST - Common Spanning Tree** - è composto da regioni MSTP che eseguono il proprio Spanning Tree tradizionale. CST utilizza i collegamenti tra gli switch al limite della zona MSTP.

CIST - Common and Internal Spanning Tree - Composto da CST e IST che attraversano più istanze in base a un mapping condiviso di VLAN all'istanza.

Lo Spanning Tree comune e interno *non* è lo Spanning Tree comune.

Ora che abbiamo stabilito a chi serve questo articolo e le definizioni pertinenti, cerchiamo di individuare le migliori pratiche.

Best Practice #1 - Verifica della necessità di eseguire la migrazione a MSTP

La prima procedura consigliata consiste nel confermare la necessità di migrare a MSTP. Uno dei fattori chiave per questa decisione è capire le prestazioni dello Spanning Tree esistente sulla rete. La migrazione al protocollo MSTP è un'ottima opzione per alcuni motivi, in quanto introduce la condivisione del carico, che determina l'impatto maggiore sull'efficienza della rete. Se il traffico di layer 2 è aumentato prima delle proiezioni, il passaggio a MSTP può aumentare l'utilità e la durata dell'ingranaggio tramite prestazioni migliorate. Altre considerazioni potrebbero essere:

Le prestazioni STP esistenti non sono soddisfacenti - il tempo di convergenza o la quantità di BPDU trasmessi causano problemi

Spanning Tree segmento: riduce il carico di risorse sugli switch contenuti nelle aree MSTP.

Ambiente hardware misto: il protocollo MSTP è uno standard aperto, ideale per ambienti di fornitori diversi. E' ampiamente sostenuta.

Nota: In genere, si ha un'idea errata quando si esegue la migrazione a Multiple Spanning Tree, è necessario mappare una VLAN per istanza.

Sono sorti sapori di Spanning Tree, con variazioni e torsioni sulle versioni precedenti. Rispetto al PVST+ (Per VLAN Spanning Tree), il protocollo MSTP utilizza meno risorse (BPDU, cicli della CPU, tempo di trasmissione) mantenendo le istanze dello Spanning Tree o le versioni logiche dello Spanning Tree. Il traffico VLAN è abilitato per passare attraverso i segmenti di layer 2 di una rete. Anche l'inoltro per una porta (e VLAN) può essere bloccato per una VLAN diversa. Inoltre, se un loop si forma in un'istanza, non influirà sulle altre istanze.

Best Practice 2: strategia della migrazione

Una volta confermata la necessità di eseguire la migrazione, è preferibile che questa venga eseguita con tempi di inattività minimi e che la connettività esistente venga preservata. Una piccola strategia per affrontare la migrazione contribuirà in modo significativo a garantire un'implementazione senza problemi. Per facilitare questo processo, si consiglia di seguire i passi tattici riportati di seguito.

1. *Documento, documento, documento:* la memorizzazione di note dettagliate consente di ridurre i tempi di migrazione e il rischio di errori.

Identificare e documentare tutte le porte point-to-point o le porte che conducono a un altro switch o router.

Identificare e documentare tutte le porte periferiche, o porte che conducono a un punto

finale come un PC o una stampante.

Definizione delle VLAN partecipanti alla migrazione

Gli stagisti sono davvero bravi in questo passo!

Determinare l'ordine delle operazioni per la rete.

Tenere presente che le modifiche apportate a uno switch possono influire su una VLAN diversa.

Pianifica il downtime della rete o esegui la migrazione nel fine settimana.

Avviare la migrazione al centro della rete e passare alla distribuzione e quindi al livello di accesso.

Best Practice n. 3 - Abilitazione delle porte point-to-point per l'utilizzo di PortFast

Questa procedura consigliata e la seguente utilizzano tutta la documentazione relativa a tale porta. Gli amministratori definiscono un parametro facoltativo sulle porte perimetrali tramite la funzionalità PortFast. PortFast impedisce l'esecuzione dello Spanning Tree su questa porta. Le porte di interfaccia switch-to-gear possono includere un server, una workstation o un router. L'intenzione è che quella porta non colleghi mai la rete a un altro gruppo di porte aperte. Il che potrebbe causare loop se lo switch riceve una BPDU superiore. Poiché le porte in linea su una rete subiscono un calcolo STP sulla porta, è possibile risparmiare tempo e carico della CPU assegnando in anticipo lo stato di blocco. Consente alla porta di passare rapidamente a uno stato di invio - inoltre BPDU. Perché lo stato è stato assegnato in anticipo.

Nota: Verificare che le porte sugli switch siano configurate per la trasmissione full-duplex.

I passaggi seguenti verranno suddivisi tra switch per PMI (CLI + GUI) e switch Enterprise Catalyst (CLI).

Abilitazione di Portfast su switch Catalyst - CLI

I comandi CLI vengono presentati per primi nella sintassi, seguiti da un esempio di comando live. È stato aggiunto uno spazio aggiuntivo dopo il simbolo # per semplificare leggermente l'evidenziazione per il comando Copia > Incolla. Il testo evidenziato in blu indica le variabili che devono essere sostituite con i dettagli contestuali della rete. Inoltre, per brevità, gli unici comandi di elevazione dei privilegi utilizzati saranno per la configurazione MSTP.

```
Catalyst(config)# interface [range(optional)] [port-id]
Catalyst(config-if)# spanning-tree portfast [auto]
```

```
Catalyst(config)# interface range fa0/1 - 24
Catalyst(config-if)# spanning-tree portfast auto
```

Abilitazione di Portfast sullo switch per PMI - CLI

```
SMBswitch(config)# interface [intervallo(facoltativo)] [id-porta]
SMBswitch(config-if)#spanning-tree portfast
```

```
SMBswitch(config)# intervallo interfaccia gi1-15
SMBswitch(config-if)# spanning-tree portfast
```

Abilitazione di Portfast sullo switch per PMI - GUI

Come si può notare, l'interfaccia utente degli switch per PMI utilizza un sinonimo di *PortFast* - è nota come *Fast Link*.

Passaggio 1. Fare clic su **Spanning Tree > Impostazioni interfaccia STP**.

Passaggio 2. Selezionare un'interfaccia e fare clic sul pulsante **Modifica**.

Passaggio 3. Fare clic su **Abilita** collegamento rapido.

Nota: Ricordarsi di applicare le modifiche e di scrivere la configurazione in esecuzione nella configurazione di avvio.

Best Practice n. 4 - Abilitazione di BPDU Guard sulle porte edge

Questa procedura ottimale è un'estensione di quella precedente. Se una porta abilitata per BPDU Guard rileva che la porta riceve qualsiasi BPDU superiore che cambia la topologia, la porta viene chiusa immediatamente tramite lo stato *err-disabled*. Per risolvere il problema, è necessario accedere allo switch.

Nota: Potrebbe sembrare una di quelle procedure ottimali che potresti ignorare. Potresti farla franca? Forse, ma per il bene del vostro futuro, fatelo così. Un commutatore errante collegato alla rete e che pompa fuori BPDU errate potrebbe provocare il potenziale arresto della rete.

Abilitazione di BPDU Guard sullo switch Catalyst - CLI

```
Catalyst(config)# interface [range(optional)] [port-id]
Catalyst(config-if)# abilitazione spanning-tree bpduguard
```

```
Catalyst(config)# interface range fa0/1 - 24
Catalyst(config-if)# abilitazione spanning-tree bpduguard
```

Abilitazione di BPDU Guard sullo switch SMB - CLI

```
SMBswitch(config)# interface [range(optional)] [port-id]
SMBswitch(config-if)# abilitazione spanning-tree bpduguard
```

```
SMBswitch(config)# interface range fa0/1 - 24
SMBswitch(config-if)# abilitazione spanning-tree bpduguard
```

Abilitazione di BPDU Guard sullo switch SMB - GUI

Passaggio 1. Accedere all'utility di configurazione Web per scegliere **Spanning Tree > Impostazioni interfaccia STP**. Viene visualizzata la pagina Impostazioni interfaccia STP.

Passaggio 2. Selezionare il tipo di **interfaccia** da modificare dall'elenco a discesa Tipo di interfaccia.

Passaggio 3. Fare clic su **Go** per visualizzare solo le porte o i LAG nella pagina.

Passaggio 4. Fare clic sul pulsante di **opzione** della porta o del LAG collegato all'altro switch e fare

clic su **Modifica**. Viene visualizzata la finestra Modifica interfaccia STP.

Passaggio 5. Selezionare la casella di controllo **Abilita** BPDU Guard corrispondente al tipo di interfaccia desiderato nel campo *Interfaccia*.

Best Practice 5: mappatura delle VLAN agli MSTI, non all'IST (MST0)

A questo punto le porte conoscono il ruolo appropriato, passare alla mappatura delle istanze. Per ottenere risultati ottimali, limitate la quantità di varianti create - tenete presente che vi sono alcune sfumature. Ciò è in contrasto con le best practice e potrebbe dissuadere un tecnico da MSTP come soluzione. È possibile avere considerazioni valide sulla progettazione della rete per più istanze, ma è consigliabile avere una singola istanza. Decidere quali VLAN mappare sulle istanze. Quindi, scegliere un nome per la configurazione e un numero di revisione che saranno comuni a tutti gli switch della rete.

Nota: Quando si modificano i mapping della VLAN MSTI, il protocollo MSTP viene riavviato.

Mappatura delle VLAN sullo switch Catalyst - CLI

```
Catalyst(config)# configurazione mst spanning-tree  
Catalyst(config-mst)# instance [instance-id] vlan [vlan-range]
```

```
Catalyst(config)# configurazione mst spanning-tree  
Catalyst(config-mst)# istanza 1 vlan 1-11
```

Mappatura delle VLAN sullo switch SMB - CLI

```
SMBswitch(config)# configurazione principale spanning-tree  
SMBswitch(config-mst)# instance [instance-id] vlan [vlan-range]
```

```
SMBswitch(config)# configurazione principale spanning-tree  
SMBswitch(config-mst)# istanza 1 vlan 1-11
```

Mappatura di VLAN su MSTI - GUI

Passaggio 1. Fare clic su **Spanning Tree > VLAN to MSTP Instance**.

La pagina *VLAN su istanza MSTP* contiene i campi riportati di seguito.

- *ID istanza MST*: vengono visualizzate tutte le istanze MSTP.
- *VLAN*: vengono visualizzate tutte le VLAN appartenenti all'istanza MST.

Passaggio 2. Per aggiungere una VLAN a un'istanza MSTP, selezionare l'**istanza MST**, quindi fare clic su **Modifica**.

- ID variante MST (MST Instance ID) - Selezionate la variante MST.
- VLAN: per definire le VLAN da mappare su questa istanza MST.
- Azione: definire se aggiungere (mappare) la VLAN all'istanza MST o rimuoverla.

Passaggio 3. Inserire i **parametri**.

Passaggio 4. Fare clic su **Applica**. A questo punto, vengono stabiliti i mapping della VLAN MSTP.

Best Practice n. 6: collocazione di tutti gli switch abilitati per

MSTP nella stessa area

La procedura ottimale consiste nel posizionare il maggior numero possibile di switch in un'unica regione. La segmentazione della rete in più regioni non presenta vantaggi. Come per qualsiasi protocollo di routing e switching, richiedono un modo per confermare l'appartenenza al protocollo. I BPDU inviati consentono a uno switch di riconoscersi come membro di una particolare regione. Affinché il bridge possa comprendere la propria appartenenza a una determinata regione, è necessario che condivida le impostazioni seguenti:

1. Nome area
2. Numero revisione
3. Digest calcolato dal mapping tra VLAN e istanza

Posizionamento del bridge all'interno di una regione sullo switch Catalyst - CLI

```
Catalyst(config)# spanning-tree mst [instance-id] principale
```

```
Catalyst(config)# spanning-tree mst 5 principale
```

Collocare il bridge all'interno di una regione sullo switch per PMI - CLI

```
SMBswitch(config)# configurazione principale spanning-tree  
SMBswitch(config-mst)# instance [instance-id] vlan [vlan-range]  
SMBswitch(config-mst)# nome [region-name]  
SMBswitch(config-mst)# revisione [ID-revisione]
```

```
SMBswitch(config)# configurazione principale spanning-tree  
SMBswitch(config-mst)# istanza 1 vlan 10-20  
SMBswitch(config-mst)# nome regione1  
SMBswitch(config-mst)# revisione 1
```

Collocare il ponte all'interno di una regione sullo switch per PMI - GUI

La pagina Proprietà MSTP viene utilizzata per definire la regione in cui si trova lo switch. Affinché i dispositivi si trovino nella stessa regione, devono avere lo stesso nome e lo stesso valore di revisione.

Passaggio 1. Scegliere **Spanning Tree > Proprietà MSTP** dal menu.

Passaggio 2. Inserire un **nome** per l'area MSTP nel campo *Nome area*. Il nome della regione definisce il limite logico della rete. Tutti gli switch in un'area MSTP devono avere lo stesso nome di area configurato.

Passaggio 3. Inserire un **numero di revisione** nel *campo Revisione*. Questo è un numero logico che indica una revisione per la configurazione MSTP. Tutti gli switch in un'area MSTP devono avere lo stesso numero di revisione.

Passaggio 4. Inserire il numero massimo di **hop** nel campo *Max hop*. Max Hops specifica la durata delle BPDU nel numero di hop. Quando un bridge riceve un pacchetto BPDU, diminuisce di uno il numero di hop e invia nuovamente il pacchetto BPDU con il nuovo numero di hop. Quando un bridge riceve una BPDU con un numero di hop pari a zero, la BPDU viene scartata.

Nota: Il campo *Attivo IST* visualizza la priorità bridge e l'indirizzo MAC dello switch attivo della regione. [Per ulteriori informazioni, vedere il glossario.](#)

Passaggio 5. Fare clic su **Applica**.

Best Practice n. 7 - Nidificare il bridge radice del CIST nell'area MST principale

Questa buona pratica è parte del processo per tenere insieme l'intera migrazione. L'idea è di posizionare il bridge radice per la topologia MSTP all'interno dell'area MSTP primaria. Data la procedura ottimale precedente che prevede l'inserimento di tutte le VLAN nella stessa regione, la selezione della radice è valida per tutte le VLAN. Ciò è possibile grazie alla funzione denominata Root Guard, che applica il posizionamento della radice creato dall'utente. Quando un bridge riceve una BPDU superiore su una porta attivata da root Guard, attiva immediatamente la porta in modalità di ascolto, tramite uno stato STP non coerente nella radice. In questo modo si impedisce l'inoltro delle BPDU inferiori e si preservano le porte designate sul ponte radice della propria area. In questo modo vengono mantenute le porte designate sul ponte principale della propria regione.

Nota: Selezionare con attenzione la radice e una radice di backup per ogni istanza.

Posizionamento del bridge radice su CIST su switch Catalyst - CLI

```
Catalyst(config)# spanning-tree mst [instance-id] root {primary | secondario} [diametro dia  
[hello-time hello-time]]
```

```
Catalyst(config)# spanning-tree mst 1 radice primaria 7
```

Risoluzione dei problemi - Catalyst

Il comando seguente restituirà il comando seguente restituirà tutte le porte contrassegnate come incoerenti. Tuttavia, il comando non è disponibile sugli switch per PMI.

```
Catalyst# show spanning-tree inconsistentports
```

Posizionamento del bridge radice sul CIST su uno switch per PMI - CLI

```
SMBswitch(config)# interface [id-interfaccia]  
Switch SMB(config-if)# spanning-tree guard root
```

```
SMBswitch(config)# interface gi1/1/1  
SMBswitch(config-if)# radice spanning-tree guard
```

Posizionamento del bridge radice sul CIST su uno switch per PMI - GUI

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Spanning Tree > Impostazioni interfaccia STP**.

Passo 2: scegliere un'**interfaccia** dall'elenco a discesa *Tipo interfaccia*.

Passaggio 3. Fare clic su **Go** per visualizzare un elenco di porte o LAG sull'interfaccia.

Passaggio 4. Fare clic sul **pulsante di opzione** della porta o **del LAG** che si desidera modificare e fare clic su **Modifica**. Viene visualizzata la finestra Modifica impostazione interfaccia STP.

Passaggio 5. Fare clic sul **pulsante di opzione** corrispondente all'interfaccia desiderata nel campo Interfaccia.

- Porta: dall'elenco a discesa Porta, scegliere la porta da configurare. Ciò influirà solo sulla singola porta scelta.

- LAG — dall'elenco a discesa LAG, scegliere il LAG da configurare. Ciò influirà sul gruppo di porte definite nella configurazione LAG.

Passaggio 6. Per abilitare STP sull'interfaccia, verificare che STP sia selezionato **Abilita** nel campo *STP*.

Passaggio 7. Selezionare **Enable** nel campo *Root Guard* per abilitare Root Guard sull'interfaccia. Questa opzione consente di applicare il posizionamento del bridge radice nella rete. Root Guard viene usato per impedire che un nuovo dispositivo connesso assuma il controllo del bridge radice.

Verifica della migrazione - È attiva questa opzione?

A questo punto, l'implementazione e la rete MSTP dovrebbero procedere di pari passo. Per gli utenti che si fidano ma verificano, è possibile verificare lo stato MSTP eseguendo un'acquisizione del frame. Confrontare quindi i risultati con la documentazione prevista.

Dopo aver eseguito l'acquisizione di un pacchetto tramite Wireshark, verranno visualizzati *Mrecords* che contengono l'ID istanza. Di seguito è riportata una schermata di *Mrecord*, prima dell'espansione per ulteriori dettagli.

```

▼ Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Multiple Spanning Tree (3)
  BPDU Type: Rapid/Multiple Spanning Tree (0x02)
  ▶ BPDU flags: 0x7c, Agreement, Forwarding, Learning, Port Role: Designated
  ▶ Root Identifier: 24576 / 0 / 24:e9:b3:78:fe:80
  Root Path Cost: 0
  ▶ Bridge Identifier: 24576 / 0 / 24:e9:b3:78:fe:80
  Port identifier: 0x8018
  Message Age: 0
  Max Age: 20
  Hello Time: 2
  Forward Delay: 15
  Version 1 Length: 0
  Version 3 Length: 96
  ▼ MST Extension
    MST Config ID format selector: 0
    MST Config name: Cisco
    MST Config revision: 1
    MST Config digest: 2a5477095c475f337a69c797b32cd60a
    CIST Internal Root Path Cost: 0
    ▶ CIST Bridge Identifier: 24576 / 0 / 24:e9:b3:78:fe:80
    CIST Remaining hops: 20
    ▶ MSTID 1, Regional Root Identifier 24576 / 24:e9:b3:78:fe:80
    ▶ MSTID 2, Regional Root Identifier 24576 / 24:e9:b3:79:06:00
  
```

MRecords

Espansione di *Mrecord* Consente di visualizzare dati più granulari su MSTP. Tra cui:

- Ruolo porta
- ID MST
- Radice regionale
- Costo percorso interno
- Priorità identificatore bridge
- Priorità identificatore porta
- Hop rimanenti

```

▼ MSTID 1, Regional Root Identifier 24576 / 24:e9:b3:78:fe:80
  ▶ MSTI flags: 0x7c, Agreement, Forwarding, Learning, Port Role: Designated
  0110 .... = Priority: 0x6
  
```

Comandi di verifica rapida - CLI per PMI

Per verificare dalla riga di comando, provare i seguenti comandi:

```
SMBswitch# show spanning-tree mst-configuration  
  
SMBswitch(config)# configurazione principale spanning-tree  
SMBswitch(config-mst)# visualizzazione in sospeso
```

Configurazione MST in sospeso

```
Name [regione1]  
Revisione 1  
Istanze configurate 2  
Vlan Istanza Mappate
```

—

```
0 1-9,21-4094
```

```
1 10-20
```

—

```
SMBswitch# show spanning-tree mst-configuration
```

```
Nome []  
Revisione 0  
Vlan istanza mappate
```

—

```
0 1-4094
```

—

Nota: la versione Catalyst del comando show esclude il segno - tra mst e configuration. EX:"show spanning-tree mst configuration"

Cosa sapere su PVST+ e MSTP che vivono sulla stessa rete

Se è necessario continuare a supportare gli switch legacy che eseguono PVST+, gestire questa operazione porta per porta. Se uno di questi switch viene eseguito come trunk VLAN, verificare che lo switch MSTP sia la radice di tutte le VLAN assegnate al trunk. Inoltre, MSTP tenta di decodificare PVST+ BPDU, ma questa simulazione è imperfetta. Il che ci richiede di tuffarci nell'idea delle porte di confine.

Il ruolo e lo stato di una porta limite MSTP vengono determinati dall'interazione dello *Spanning Tree interno* con la topologia esterna. Ciò significa che se una porta è in modalità di blocco nell'*elenco* delle porte, viene bloccata in tutte le istanze di MSTP. Questo effetto si propaga all'implementazione PVST+, influenzando sulla funzione VLAN. Lo stesso vale se la porta è in fase di inoltro, apprendimento, ecc. Come potete immaginare, questo può diventare un problema. Ciò può causare un problema non risolvibile, mentre una porta che deve inoltrare una VLAN sta invece bloccando l'accesso a causa delle esigenze di un'altra VLAN. La simulazione PVST+ sfrutta le informazioni dell'*IST* per creare BPDU per VLAN. Il risultato è un'"illusione" a livello di rete che la regione MSTP venga visualizzata come un unico switch per tutte le VLAN. Analogamente alla modalità di *impilamento* degli switch, che non è male a metà. Il problema, nella posizione della porta di confine, è che crea la necessità di inviare singoli BPDU per ciascuna VLAN simulata. Qualsiasi incoerenza tra le BPDU può compromettere l'intera simulazione in termini di errori. Solo la ricezione di BPDU consistenti consentirà alla simulazione di farsi da parte.

Per concludere, l'intera situazione spiega perché i BPDU ricevuti sulla porta di confine devono essere identici. [Per ulteriori informazioni su questo argomento, fare riferimento a questo thread della community.](#)

C'è qualcosa da sapere, se l'hardware di rete...non è interamente Cisco?

MSTP è compatibile con le versioni precedenti. Se l'hardware non Cisco supporta Rapid Spanning Tree, va tutto bene. In caso di problemi, [rivolgersi alla community di switching](#).

Conclusioni

Grazie per aver letto questa guida, con queste best practice si dovrebbe essere impostati per migliorare le prestazioni della rete di layer 2.

È importante notare che Spanning Tree potrebbe non sembrare un'esperienza entusiasmante, ma i vantaggi della condivisione del carico rendono la soluzione ideale per mantenere efficiente la rete. La creatrice di Spanning Tree, Radia Perlman, lo ama quanto una madre potrebbe mai. Lei ci ha anche scritto una .