

# Configurazione di Catalyst Switched Port Analyzer (SPAN): esempio

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Catalyst switch compatibili con SPAN, RSPAN ed ERSPAN](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Breve descrizione dello SPAN](#)

[Terminologia SPAN](#)

[Caratteristiche della porta di origine](#)

[Caratteristiche della VLAN di origine](#)

[Caratteristiche della porta di destinazione](#)

[Caratteristiche della porta reflector](#)

[SPAN sui Catalyst Express 500/520](#)

[SPAN sui Catalyst 2900XL/3500XL Switch](#)

[Funzioni disponibili e limitazioni](#)

[Esempio di configurazione](#)

[Esempio di rete](#)

[Esempio di configurazione sui Catalyst 2900XL/3500XL](#)

[Spiegazione della procedura di configurazione](#)

[SPAN sui Catalyst 2948G-L3 e 4908G-L3](#)

[SPAN sui Catalyst 8500](#)

[SPAN sui Catalyst serie 2900, 4500/4000, 5500/5000 e 6500/6000 Switch con CatOS](#)

[SPAN locale](#)

[PSPAN, VSPAN: monitorare alcune porte o un'intera VLAN](#)

[Monitoraggio di una porta con lo SPAN](#)

[Monitoraggio di più porte con lo SPAN](#)

[Monitoraggio delle VLAN con lo SPAN](#)

[SPAN in ingresso/in uscita](#)

[Implementazione dello SPAN su un trunk](#)

[Monitoraggio di un sottogruppo di VLAN appartenenti a un trunk](#)

[Trunking sulla porta di destinazione](#)

[Creazione di più sessioni simultanee](#)

[Altre opzioni SPAN](#)

[RSPAN \(Remote SPAN\)](#)

[Panoramica di RSPAN](#)

[Esempio di configurazione dell'analizzatore RSPAN](#)

[Impostazione del trunk ISL tra i due switch S1 e S2](#)

[Creazione della RSPAN VLAN](#)

[Configurazione della porta 5/2 dello switch S2 come porta di destinazione RSPAN](#)

---

[Configurazione di una porta di origine RSPAN sullo switch S1](#)

[Verifica della configurazione](#)

[Altre configurazioni possibili con il comando set rspan](#)

[Riepilogo delle funzioni e limitazioni](#)

[SPAN sui Catalyst serie 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E Switch](#)

[SPAN sui Catalyst serie 4500/4000 e Catalyst serie 6500/6000 Switch con software di sistema Cisco IOS](#)

[Esempio di configurazione](#)

[Riepilogo delle funzioni e limitazioni](#)

[Conseguenze sulle prestazioni dello SPAN sulle diverse piattaforme Catalyst](#)

[Catalyst serie 2900XL/3500XL](#)

[Panoramica dell'architettura](#)

[Conseguenze sulle prestazioni](#)

[Catalyst serie 4500/4000](#)

[Panoramica dell'architettura](#)

[Conseguenze sulle prestazioni](#)

[Catalyst serie 5500/5000 e 6500/6000](#)

[Panoramica dell'architettura](#)

[Conseguenze sulle prestazioni](#)

[Domande frequenti e problemi comuni](#)

[Problemi di connettività causati da un'errata configurazione dello SPAN](#)

[Stato attivo/inattivo della porta SPAN di destinazione](#)

[Perché la sessione SPAN crea un bridging loop?](#)

[Lo SPAN influisce sulle prestazioni?](#)

[È possibile configurare lo SPAN su una porta EtherChannel?](#)

[È possibile eseguire più sessioni SPAN allo stesso tempo?](#)

[Errore limite delle sessioni locali superato](#)

[Impossibile eliminare una sessione SPAN sul modulo di servizio VPN perché in uso](#)

[Perché non è possibile acquisire pacchetti danneggiati con lo SPAN?](#)

[Errore: % sessione 2 utilizzata dal modulo del servizio](#)

[Eliminazione dei pacchetti sulla porta reflector](#)

[Sui Catalyst 6500 la sessione SPAN viene usata sempre con un modulo FWSM](#)

[È possibile usare lo stesso ID per una sessione SPAN e una sessione RSPAN nello stesso switch?](#)

[È possibile eseguire una sessione RSPAN su domini VTP diversi?](#)

[È possibile eseguire una sessione RSPAN su WAN o reti diverse?](#)

[È possibile avere contemporaneamente una sessione RSPAN di origine e di destinazione sullo stesso Catalyst Switch?](#)

[Impossibile raggiungere l'analizzatore di rete o il dispositivo di sicurezza connesso alla porta SPAN di destinazione](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento vengono descritte alcune funzionalità di Switched Port Analyzer (SPAN) recentemente implementate.

# Prerequisiti

## Catalyst switch compatibili con SPAN, RSPAN ed ERSPAN

Catalyst switch	Supporto SPAN	Supporto RSPAN	Supporto ERSPAN
Catalyst Express serie 500 / 520	Sì	No	No
Catalyst serie 6500/6000	Sì	Sì	Sì. Supervisor 2T con PFC4, Supervisor 720 con PFC3B o PFC3BXL con Cisco IOS Software Release 12.2(18)SXE o versioni successive. Supervisor 720 con PFC3A con versione hardware 3.2 o successive e con Cisco IOS Software Release 12.2(18)SXE o versioni successive.
Catalyst serie 5500/5000	Sì	No	No
Catalyst serie 4900	Sì	Sì	No
Catalyst serie 4500/4000 (include 4912G)	Sì	Sì	No
Catalyst serie 3750 Metro	Sì	Sì	No
Catalyst serie 3750 / 3750E /3750X	Sì	Sì	No
Catalyst serie 3560 / 3560E/ 3650X	Sì	Sì	No
Catalyst serie 3550	Sì	Sì	No
Catalyst serie 3500 XL	Sì	No	No
Catalyst serie 2970	Sì	Sì	No
Catalyst serie 2960	Sì	Sì	No
Catalyst serie 2955	Sì	Sì	No
Catalyst serie 2950	Sì	Sì	No

Catalyst serie 2940	Sì	No	No
Catalyst 2948G-L3	No	No	No
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	Sì	Sì	No
Catalyst serie 2900XL	Sì	No	No
Catalyst serie 1900	Sì	No	No

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

In questo documento, si fa riferimento ai Catalyst serie 4500/4000, 5500/5000 e 6500/6000 Switch con CatOs 5.5. Sui Catalyst serie 2900XL/3500XL Switch, viene usato Cisco IOS® Software Release 12.0(5)XU.

Sebbene questo documento sia stato aggiornato per riflettere le modifiche apportate alla funzione SPAN, consultare le note sulla versione della documentazione della piattaforma in uso per gli sviluppi più recenti.

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.

## Premesse

La funzionalità SPAN, denominata a volte mirroring delle porte o monitoraggio delle porte, seleziona il traffico di rete per farlo esaminare da un analizzatore di rete. L'analizzatore di rete può essere un dispositivo Cisco SwitchProbe o altro probe Remote Monitoring (RMON).

In precedenza, SPAN era una funzionalità relativamente base sugli switch Cisco della serie Catalyst. Tuttavia, le ultime release di Catalyst OS (CatOS) ha introdotto notevoli miglioramenti e molte nuove opzioni ora disponibili per l'utente finale.

Questo documento non vuole essere una guida di configurazione alternativa della funzione SPAN. Cerchiamo semplicemente di rispondere alle domande più comuni su questo argomento, ad esempio:

- Cos'è lo SPAN e come deve essere configurato?

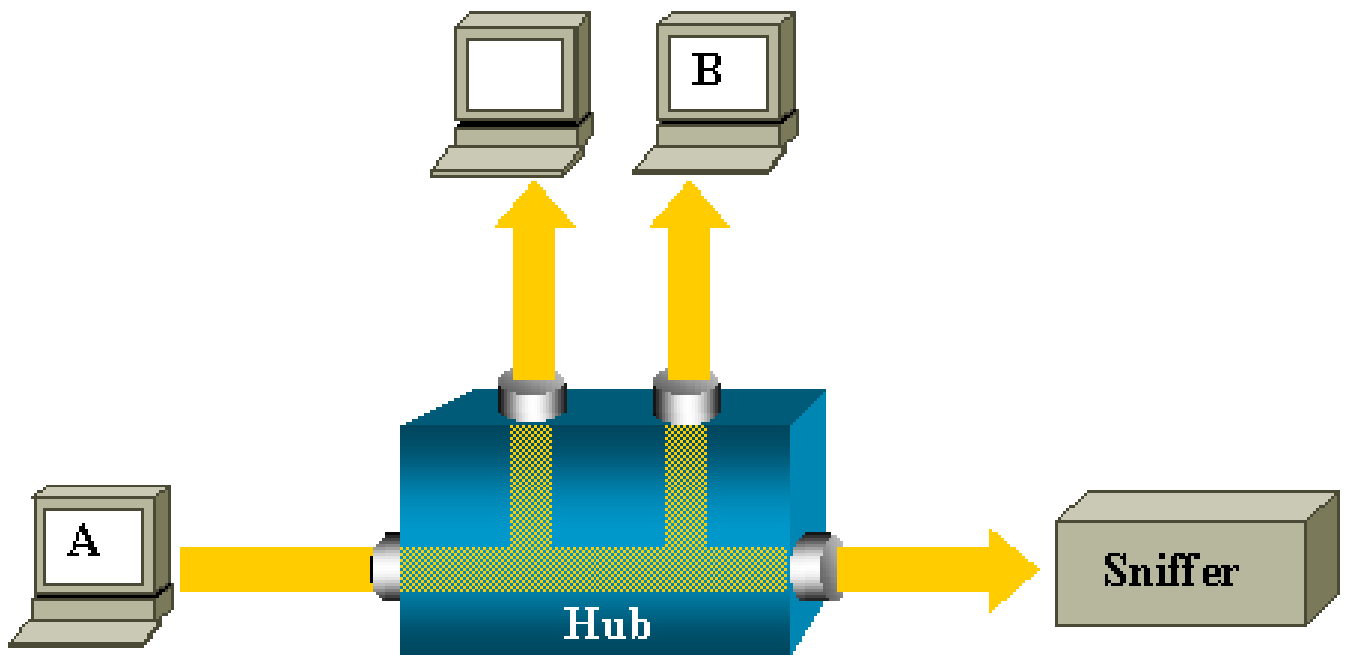
- Quali sono le diverse funzioni disponibili (in particolare è possibile avere più sessioni SPAN allo stesso tempo)? Quale versione software ne supporta l'esecuzione?
- Lo SPAN influisce sulle prestazioni dello switch?

## Breve descrizione dello SPAN

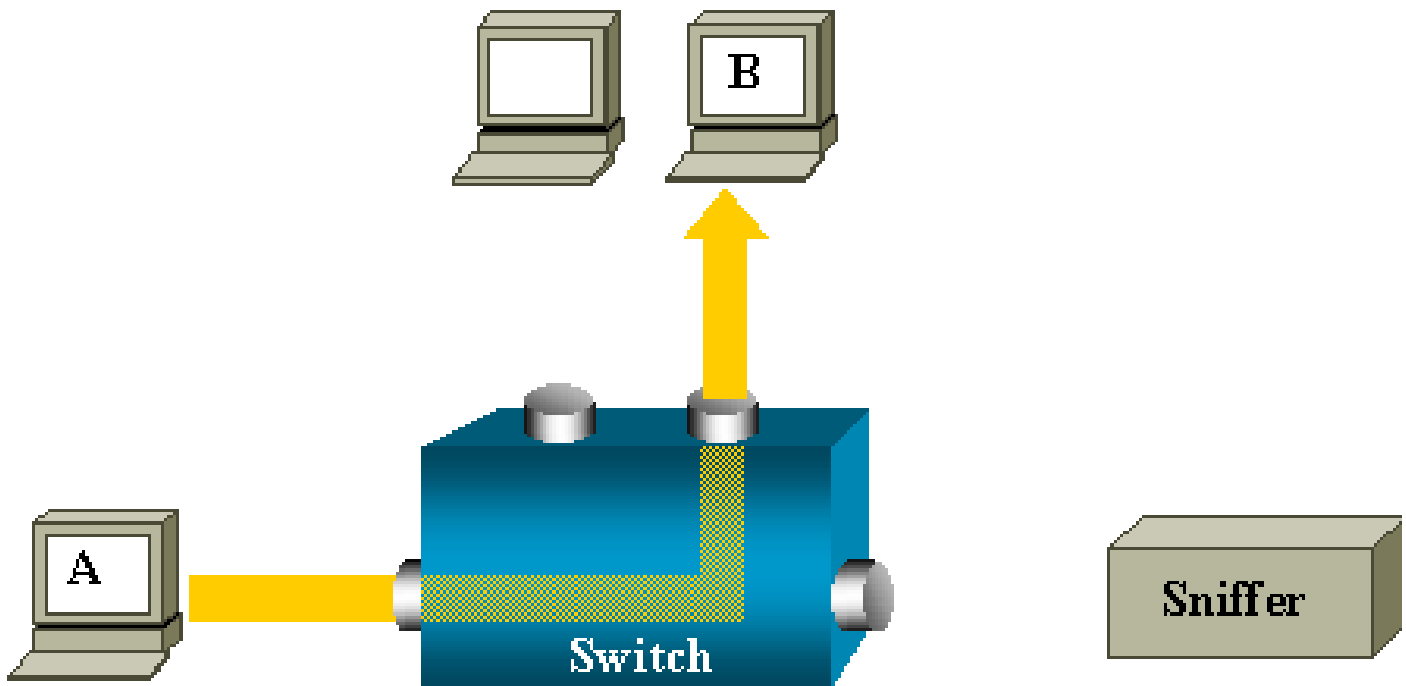
La funzione SPAN è stata introdotta sugli switch a causa del loro diverso funzionamento rispetto agli hub. Quando un hub riceve un pacchetto su una porta, ne invia una copia a tutte le porte, tranne quella su cui lo ha ricevuto.

Lo switch invece, dopo l'avvio, inizia a creare una tabella di inoltro di layer 2 sulla base dell'indirizzo MAC di origine dei diversi pacchetti ricevuti. Dopo aver creato la tabella di inoltro, lo switch inoltra il traffico direttamente alla porta che lo deve ricevere in base all'indirizzo MAC.

Ad esempio, per acquisire il traffico Ethernet inviato dall'host A all'host B ed entrambi sono collegati a un hub, è sufficiente collegare uno sniffer a questo hub. Tutte le porte possono visualizzare i dati scambiati tra gli host A e B:



Su uno switch, dopo aver acquisito l'indirizzo MAC dell'host B, il traffico unicast tra A e B viene inoltrato solo alla porta dell'host B. Pertanto, lo sniffer non può vedere questo traffico:



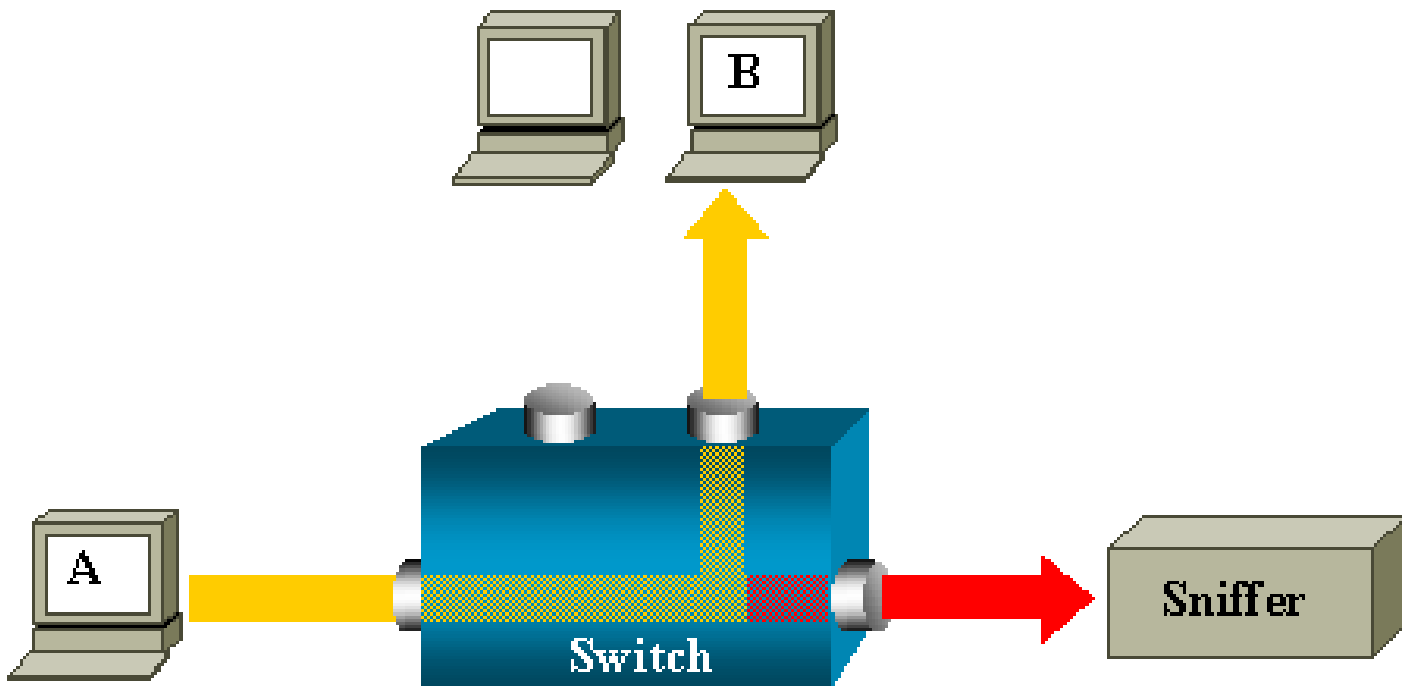
In questa configurazione, lo sniffer acquisisce solo il traffico inoltrato a tutte le porte, ad esempio:

- Traffico broadcast
- Traffico multicast con snooping CGMP o IGMP (Internet Group Management Protocol) disabilitato
- Traffico unknown unicast

L'inoltro del traffico unicast a tutte le porte è possibile solo se la tabella CAM (Content Addressable Memory) dello switch non contiene l'indirizzo MAC di destinazione.

Lo switch quindi non sa dove inviare il traffico e invia i pacchetti a tutte le porte della VLAN di destinazione.

È quindi necessaria una funzionalità aggiuntiva che copi in modo artificiale i pacchetti unicast inviati alla porta dello sniffer dall'host A:

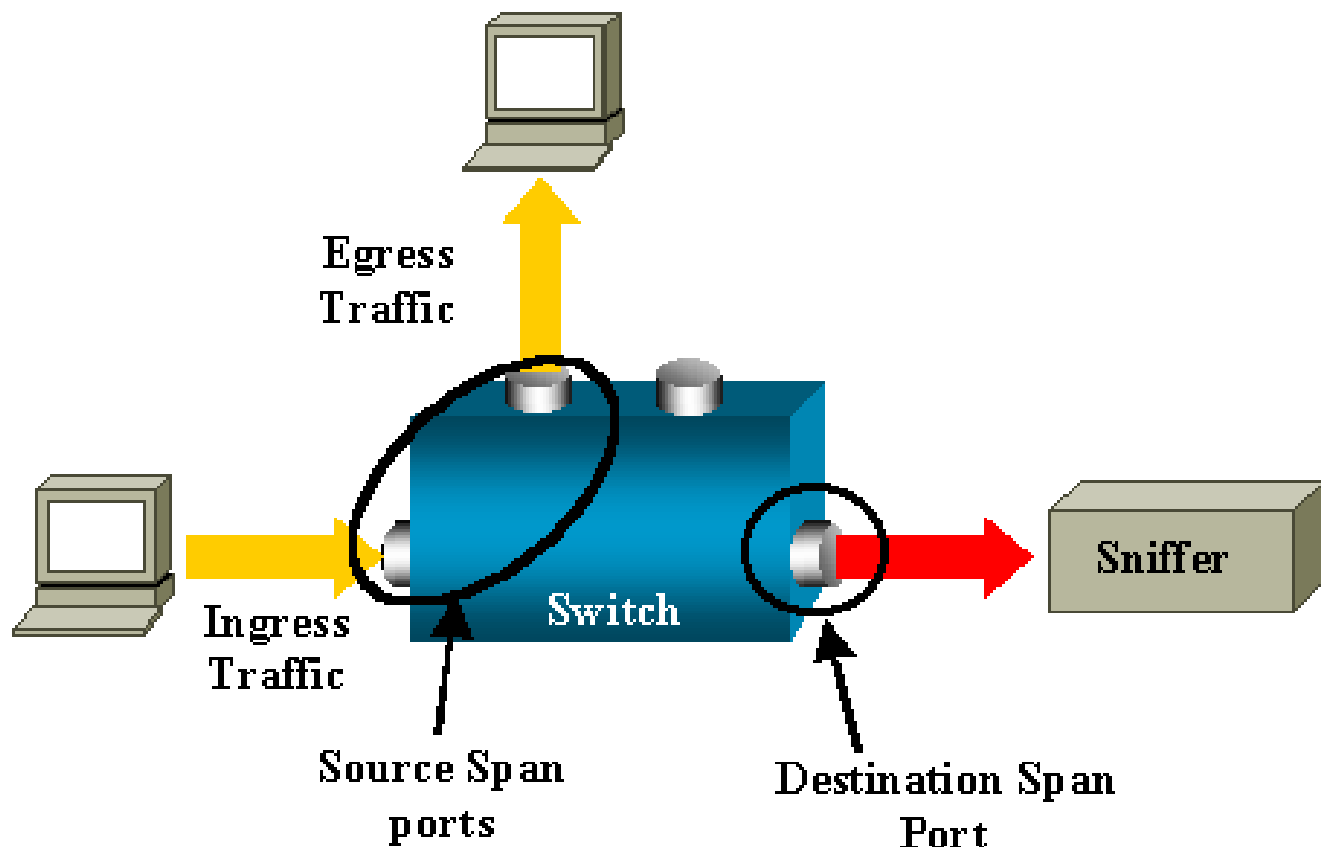


In questo schema, lo sniffer è collegato a una porta configurata per ricevere la copia di ciascun pacchetto inviato dall'host A. Questa porta è chiamata porta SPAN.

Nel prosieguo di questo documento viene descritto in dettaglio come ottimizzare la funzione in modo che possa svolgere altre attività oltre al monitoraggio della porta.

## Terminologia SPAN

- Traffico in ingresso: traffico in arrivo nello switch.
- Traffico in uscita: traffico in partenza dallo switch.
- [Porta \(SPAN\) di origine](#) : una porta monitorata con la funzione SPAN.
- [VLAN \(SPAN\) di origine](#): una VLAN il cui traffico è monitorato dalla funzione SPAN.
- [Porta \(SPAN\) di destinazione](#): una porta che monitora le porte di origine, a cui in genere è collegato un analizzatore di rete.
- [Porta reflector](#): una porta su cui vengono copiati i pacchetti trasmessi sulla RSPAN VLAN.
- Porta di monitoraggio: nella terminologia dei Catalyst 2900XL/3500XL/2950 Switch, una porta di monitoraggio è anche una porta SPAN di destinazione.



- SPAN locale: la funzione SPAN è locale quando le porte monitorate si trovano tutte sullo stesso switch della porta di destinazione. Questa funzione è opposta alla funzione Remote SPAN (RSPAN), descritta più avanti.
- Remote SPAN (RSPAN): alcune porte di origine non condividono lo stesso switch della porta di destinazione.

RSPAN è una funzionalità avanzata che richiede la creazione di una VLAN speciale a cui trasmettere il traffico tra gli switch monitorato dallo SPAN.

La funzione RSPAN non è supportata su tutti gli switch. Consultare le note sulla versione o la guida alla configurazione del modello in uso per verificare se la funzione RSPAN può essere usata.

- SPAN basato sulle porte, o PSPAN (Port-based SPAN): l'utente specifica una o più porte di origine sullo switch e una porta di destinazione.
- SPAN basato sulla VLAN, o VSPAN (VLAN-based SPAN): su un determinato switch, l'utente può scegliere di monitorare tutte le porte che appartengono a una determinata VLAN con un unico comando.
- ESPAN: sta per "enhanced SPAN", ossia una versione SPAN migliorata. Questo termine è stato utilizzato diverse volte durante l'evoluzione dell'SPAN al fine di denominare le caratteristiche aggiuntive, quindi, il termine non è molto chiaro ed è evitato in questo documento.
- Origine amministrativa: un elenco di porte o VLAN di origine configurate per essere



monitorate.

- Origine operativa: un elenco di porte effettivamente monitorate. Questo elenco di porte può essere diverso dall'origine amministrativa.

Ad esempio, una porta in modalità di spegnimento può apparire come origine amministrativa, ma non essere nella realtà oggetto di monitoraggio.

## Caratteristiche della porta di origine

Per porta di origine, o porta monitorata, si intende la porta di uno switch o di un router su cui viene monitorato il traffico di rete per successive analisi.

In una sessione SPAN locale o in una sessione RSPAN di origine, è possibile monitorare il traffico ricevuto (Rx) sulla porta di origine, il traffico trasmesso (Tx) o il traffico in entrambe le direzioni.

Lo switch supporta un numero qualsiasi di porte di origine (fino al numero massimo di porte disponibili sullo switch) e un numero qualsiasi di VLAN di origine.

Caratteristiche di una porta di origine:

- Può essere qualsiasi tipo di porta, EtherChannel, Fast Ethernet, Gigabit Ethernet e così via.
- Può essere monitorata in più sessioni SPAN.
- Non può essere una porta di destinazione.
- Su ciascuna porta di origine è possibile configurare una direzione di monitoraggio (in ingresso, in uscita o in entrambe le direzioni). Sulle porte di origine EtherChannel, la direzione monitorata si applica a tutte le porte fisiche del gruppo.
- Le porte di origine possono trovarsi nella stessa VLAN o in VLAN diverse.
- Sulle porte di origine VLAN SPAN, tutte le porte attive nella VLAN di origine sono considerate porte di origine.

## Filtro VLAN

Quando la porta di origine monitorata è una porta trunk, vengono monitorate per impostazione predefinita tutte le VLAN attive sul trunk. Il filtro VLAN serve a limitare il monitoraggio del traffico SPAN sulle porte di origine trunk a VLAN specifiche.

- Il filtro VLAN si applica solo alle porte trunk o alle porte di VLAN voce.
- Il filtro VLAN si applica solo alle sessioni basate sulle porte e non è consentito nelle sessioni con origini VLAN.
- Quando viene specificato un elenco di filtri VLAN, solo le VLAN menzionate nell'elenco vengono monitorate sulle porte trunk o sulle porte di accesso alle VLAN voce.

- Il traffico SPAN proveniente da altri tipi di porta non è influenzato dal filtro VLAN, sulle altre porte sono quindi consentite tutte le VLAN.
- Il filtro VLAN influisce solo sul traffico inoltrato alla porta SPAN di destinazione e non influisce sulla commutazione del traffico normale.
- Non è possibile avere in un'unica sessione VLAN di origine e VLAN filtrate. È possibile avere VLAN di origine o VLAN filtrate, ma non entrambe contemporaneamente.

## Caratteristiche della VLAN di origine

VSPAN permette il monitoraggio del traffico di rete in una o più VLAN. In VSPAN, l'interfaccia SPAN o RSPAN di origine è un ID VLAN; il traffico viene monitorato su tutte le porte di tale VLAN.

Caratteristiche di VSPAN:

- Tutte le porte attive nella VLAN di origine sono considerate porte di origine e possono essere monitorate in una o in entrambe le direzioni.
- Su una data porta, solo il traffico della VLAN monitorata viene inviato alla porta di destinazione.
- Se una porta di destinazione appartiene a una VLAN di origine, viene esclusa dall'elenco di origine e non viene monitorata.
- Se si aggiungono o rimuovono porte da una VLAN di origine, il traffico ricevuto su tali porte viene rispettivamente aggiunto o rimosso dalle origini che sono monitorate.
- Non è possibile usare le VLAN filtrate nella stessa sessione delle VLAN di origine.
- È possibile monitorare solo VLAN Ethernet.

## Caratteristiche della porta di destinazione


In ogni sessione SPAN o RSPAN di destinazione locale deve essere presente una porta di destinazione (o porta di monitoraggio) su cui viene copiato il traffico trasmesso dalle porte di origine e dalle VLAN.

Caratteristiche della porta di destinazione:


- Una porta di destinazione deve risiedere sullo stesso switch della porta di origine (per una sessione SPAN locale).
- Una porta di destinazione può essere qualsiasi porta fisica Ethernet.
- Una porta di destinazione può partecipare a una sola sessione SPAN alla volta. La porta di destinazione di una sessione SPAN non può essere anche la porta di destinazione di un'altra sessione SPAN.
- Una porta di destinazione non può essere una porta di origine.

- Una porta di destinazione non può essere un gruppo EtherChannel.

---

 Nota: dal software Cisco IOS versione 12.2(3)SXH e successive, l'interfaccia PortChannel può essere una porta di destinazione. EtherChannel di destinazione non supporta il protocollo PAgP (Port Aggregation Control Protocol) o il protocollo LACP (Link Aggregation Control Protocol) EtherChannel. È supportata solo la modalità on, con tutto il supporto del protocollo EtherChannel disabilitato.


---

 Nota: per ulteriori informazioni, fare riferimento alle [destinazioni Local SPAN, RSPAN ed ERSPAN](#).

---

- È possibile usare come porta di destinazione una porta fisica assegnata a un gruppo EtherChannel, anche se il gruppo EtherChannel è stato specificato come SPAN di origine. Se configurata come porta SPAN di destinazione, la porta viene rimossa dal gruppo.
- A meno che non sia abilitata la modalità di apprendimento, sulla porta non viene trasmesso alcun traffico eccetto quello richiesto dalla sessione SPAN. Se la modalità di apprendimento è abilitata, la porta trasmette anche il traffico diretto agli host che sono stati appresi sulla porta di destinazione.

---

 Nota: per ulteriori informazioni, fare riferimento alle [destinazioni Local SPAN, RSPAN ed ERSPAN](#).

---

- Per impostazione predefinita, lo stato della porta di destinazione è attivo/inattivo. L'interfaccia mostra lo stato inattivo per evidenziare che al momento la porta non può essere usata come porta di produzione.
- Se è stato abilitato l'inoltro del traffico in ingresso per un dispositivo di sicurezza della rete, la porta di destinazione inoltra il traffico sul layer 2.
- Quando la sessione SPAN è attiva, la porta di destinazione non è interessata dal protocollo Spanning Tree.
- Se la porta è una porta di destinazione, non è interessata da nessuno dei protocolli di layer 2 (STP, VTP, CDP, DTP, PagP).
- Una porta di destinazione che appartiene a una VLAN di origine di qualsiasi sessione SPAN viene esclusa dall'elenco di origine e non viene monitorata.
- Una porta di destinazione riceve copia del traffico inviato e ricevuto su tutte le porte di origine monitorate. Se una porta di destinazione viene usata oltre la sua capacità, può crearsi una congestione. Questa congestione può influire sull'inoltro del traffico su una o più porte di origine.

## Caratteristiche della porta reflector

La porta reflector permette di copiare i pacchetti su una RSPAN VLAN. La porta reflector inoltra il traffico esclusivamente dalla sessione RSPAN di origine a cui è associata.

Qualsiasi dispositivo collegato a una porta configurata come porta reflector perde la connettività finché la sessione RSPAN di origine non è disabilitata.

Caratteristiche della porta reflector:

- È una porta impostata sul loopback.
- Non può appartenere a un gruppo EtherChannel, non può essere una porta trunk e non può essere usata per filtrare i protocolli.
- Può essere una porta fisica assegnata a un gruppo EtherChannel, anche se il gruppo EtherChannel è specificato come SPAN di origine. Se configurata come porta reflector, viene rimossa dal gruppo.
- Una porta usata come porta reflector non può essere una porta SPAN di origine o di destinazione, né può essere una porta reflector per più di una sessione alla volta.
- È invisibile a tutte le VLAN.
- La RSPAN VLAN è la VLAN nativa del traffico di loopback su una porta reflector.
- La porta reflector indirizza nuovamente allo switch il traffico senza tag. Il traffico entra quindi nella RSPAN VLAN e viene inoltrato a tutte le porte trunk su cui è presente la RSPAN VLAN.
- Il protocollo Spanning Tree viene automaticamente disabilitato sulla porta reflector.
- Alla porta reflector viene inoltrata una copia del traffico inviato e ricevuto su tutte le porte di origine monitorate.

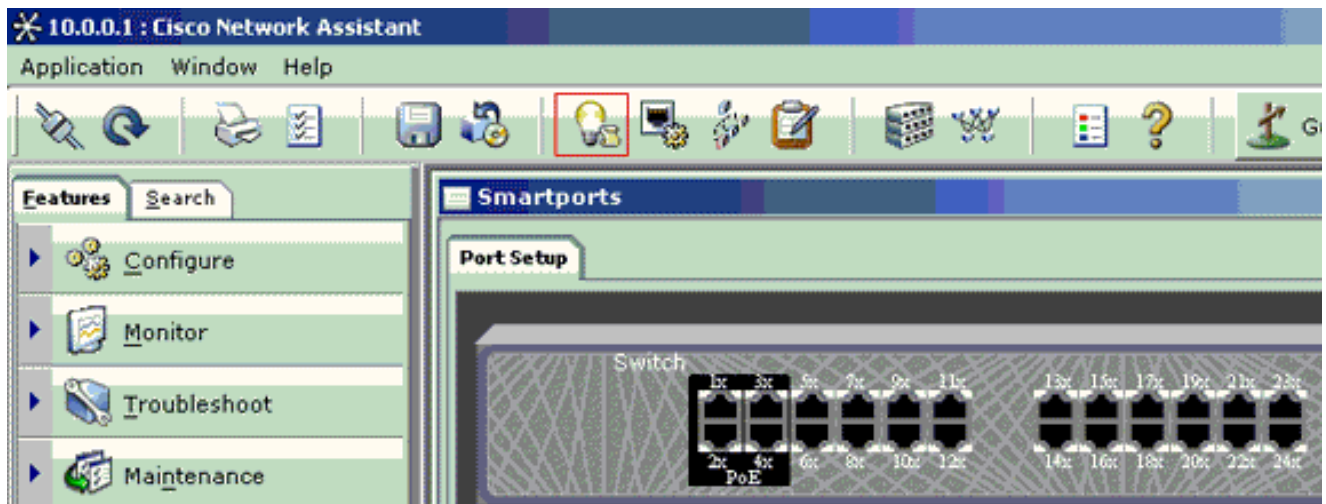
## SPAN sui Catalyst Express 500/520

Sui Catalyst Express 500 o Catalyst Express 520 è supportata solo la funzione SPAN. Per configurare lo SPAN sulle porte dei Catalyst Express 500/520, è necessario usare Cisco Network Assistant (CNA). Completare la seguente procedura per configurare lo SPAN:

1. Scaricare e installare CNA sul PC.

CNA può essere scaricato dalla pagina [Download Software](#) (Scarica software) solo dagli utenti registrati.

2. Completare la procedura descritta nella [Guida introduttiva per gli switch Catalyst Express 500](#) nella versione [12.2\(25\)FY](#) per personalizzare le impostazioni dello switch Catalyst Express 500. per ulteriori informazioni su Catalyst Express 520, fare riferimento alla [Guida introduttiva agli switch Catalyst Express 520](#).
3. Accedere allo switch con CNA, quindi fare clic su Smartport (Porta smart).

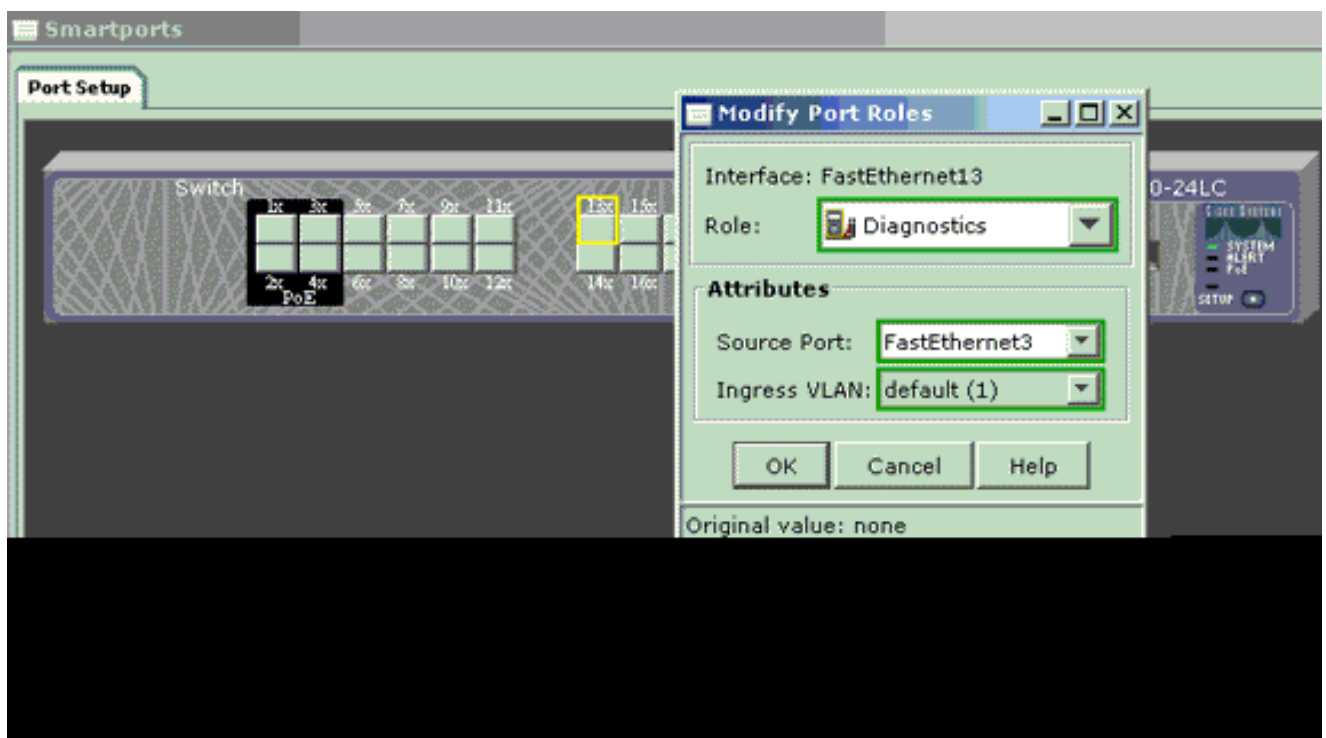


4. Fare clic su un'interfaccia a cui si desidera collegare il PC per acquisire le tracce dello sniffer.
5. Fare clic su Modify (Modifica).

Viene visualizzata una piccola finestra a comparsa.

6. Scegliere il ruolo Diagnostics (Diagnostica) per la porta.
7. Scegliere la porta di origine, quindi selezionare la VLAN che si desidera monitorare.

Se si seleziona None (Nessuna), sulla porta il traffico verrà solo ricevuto. La VLAN di ingresso consente al PC collegato alla porta di diagnostica di inviare i pacchetti alla rete che utilizza tale VLAN.



8. Fare clic su OK per chiudere la finestra a comparsa.
9. Fare clic su OK e su Apply (Applica) per applicare le impostazioni.
10. Dopo aver configurato la porta di diagnostica, è possibile usare qualsiasi software sniffer per

monitorare il traffico.

## SPAN sui Catalyst 2900XL/3500XL Switch

### Funzioni disponibili e limitazioni


La funzionalità di monitoraggio delle porte non è così estesa sui Catalyst 2900XL/3500XL ed è quindi relativamente facile da capire.

È possibile creare tutte le sessioni PSPAN locali desiderate. Ad esempio, è possibile creare sessioni PSPAN sulla porta di configurazione scelta come porta SPAN di destinazione. In questo caso, usare l'[interfaccia port monitor](#) per elencare le porte di origine che si desidera monitorare. Sui Catalyst 2900XL/3500XL, una porta di monitoraggio è definita come porta SPAN di destinazione.

- Considerare che tutte le porte relative a una determinata sessione (di origine o di destinazione) devono appartenere alla stessa VLAN.
- Se si configura l'interfaccia VLAN con un indirizzo IP, il comando port monitor monitora solo il traffico destinato all'indirizzo IP. Inoltre, monitora il traffico broadcast ricevuto dall'interfaccia VLAN. Tuttavia, non acquisisce il traffico che attraversa la VLAN stessa. Se non si specifica alcuna interfaccia per il comando port monitor, vengono monitorate tutte le altre porte che appartengono alla stessa VLAN dell'interfaccia.

Nell'elenco che segue vengono discusse alcune limitazioni. Per ulteriori informazioni, consultare la guida di riferimento ai comandi (Catalyst 2900XL/3500XL).

---

 Nota: le porte ATM sono le uniche porte che non possono essere monitorate. Una porta ATM può solo essere monitorata. Le limitazioni nell'elenco si riferiscono alle porte che hanno funzionalità di monitoraggio.

---

- Una porta di monitoraggio non può appartenere a un gruppo di porte Fast EtherChannel o Gigabit EtherChannel.
- Non è possibile abilitare la sicurezza su una porta di monitoraggio.
- Una porta di monitoraggio non può essere una porta multi VLAN.
- Una porta di monitoraggio deve appartenere alla stessa VLAN della porta monitorata. Non è consentito modificare l'appartenenza alla VLAN sulle porte di monitoraggio e sulle porte monitorate.
- Una porta di monitoraggio non può essere una porta ad accesso dinamico o una porta trunk. Tuttavia, una porta ad accesso statico può monitorare una VLAN su un trunk, una multi VLAN o una porta ad accesso dinamico. La VLAN monitorata è quella associata alla porta ad accesso statico.

- Il monitoraggio delle porte non funziona se sia la porta di monitoraggio che la porta monitorata sono protette.

Tenere presente che la porta in stato di monitoraggio non esegue lo Spanning Tree Protocol (STP) se appartiene alla stessa VLAN delle porte di cui effettua il mirroring. La porta di monitoraggio può far parte di un loop se, ad esempio, viene connessa a un hub o a un bridge collegato a un altro punto della rete. In questo caso, può verificarsi un bridging loop irreversibile perché viene a mancare la protezione del protocollo STP. Per un esempio di come questa condizione può verificarsi, vedere la sezione [Perché la sessione SPAN crea un loop di bridging?](#) di questo documento.

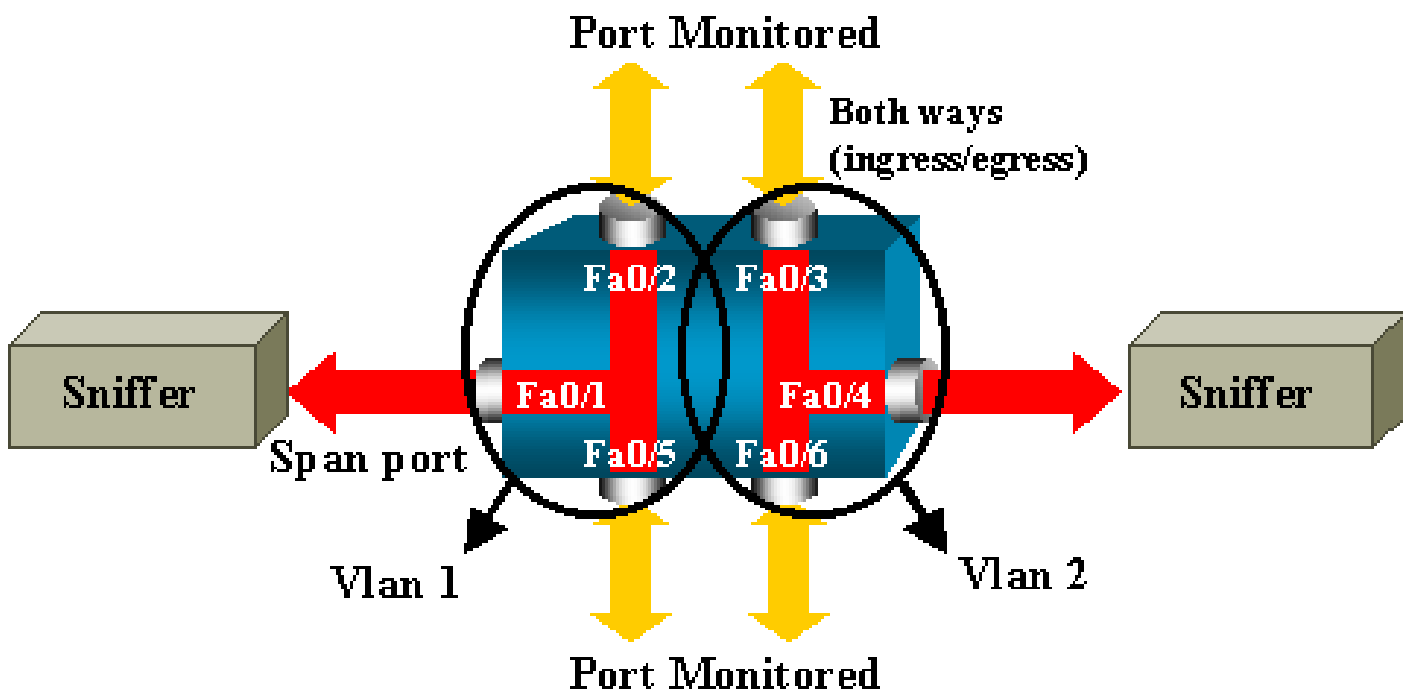
## Esempio di configurazione

Nell'esempio vengono create due sessioni SPAN simultanee.

- La porta Fast Ethernet 0/1 (Fa0/1) monitora il traffico trasmesso sulle porte Fa0/2 e Fa0/5 in entrambe le direzioni. La porta Fa0/1 monitora anche il traffico trasmesso sull'interfaccia di gestione VLAN 1.
- La porta Fa0/4 monitora le porte Fa0/3 e Fa0/6.

Le porte Fa0/3, Fa0/4 e Fa0/6 sono tutte configurate nella VLAN 2. Le altre porte e l'interfaccia di gestione sono configurate nella VLAN predefinita 1.

## Esempio di rete



## Esempio di configurazione sui Catalyst 2900XL/3500XL

Esempio di configurazione dello SPAN sui 2900XL/3500XL

```

!--- Output suppressed.
!
interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/5
port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
port monitor FastEthernet0/3
port monitor FastEthernet0/6
switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 2
!
!--- Output suppressed.
!
interface VLAN1
ip address 10.200.8.136 255.255.252.0
no ip directed-broadcast
no ip route-cache
!
!--- Output suppressed.

```

## Spiegazione della procedura di configurazione

Per configurare la porta Fa0/1 come porta di destinazione, le porte di origine Fa0/2 e Fa0/5 e l'interfaccia di gestione (VLAN 1), selezionare l'interfaccia Fa0/1 in modalità di configurazione:

```
<#root>
```

```
Switch(config)#
```

```
interface fastethernet 0/1
```

Immettere l'elenco delle porte da monitorare:

```
<#root>
```

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

```
port monitor fastethernet 0/2
```

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



```
port monitor fastethernet 0/5
```


Con questo comando, ogni pacchetto ricevuto o trasmesso da queste due porte viene copiato anche sulla porta Fa0/1. Usare una variante del comando port monitor per configurare il monitoraggio dell'interfaccia amministrativa:

```
<#root>
```

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

```
port monitor vlan 1
```

---

 Nota: questo comando non significa che la porta Fa0/1 controlli l'intera VLAN 1. la parola chiave vlan 1 si riferisce semplicemente all'interfaccia amministrativa dello switch.

---

Questo comando di esempio mostra come non sia possibile specificare una VLAN diversa per il monitoraggio di una porta:

```
<#root>
```

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

```
port monitor fastethernet 0/3
```

```
FastEthernet0/1 and FastEthernet0/3 are in different vlan
```

Per completare la procedura, configurare un'altra sessione. In questo caso, specificare la porta Fa0/4 come porta SPAN di destinazione.

```
<#root>
```

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

```
interface fastethernet 0/4
```

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

```
port monitor fastethernet 0/3
```

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

```
port monitor fastethernet 0/6
```

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

```
^Z
```

Usare il comando show running o il comando show port monitor per verificare la configurazione:


```
<#root>
```

```
Switch#
```

```
show port monitor
```

```
Monitor Port Port Being Monitored
-----
FastEthernet0/1 VLAN1
FastEthernet0/1 FastEthernet0/2
FastEthernet0/1 FastEthernet0/5
FastEthernet0/4 FastEthernet0/3
FastEthernet0/4 FastEthernet0/6
```

---

 Nota: gli switch Catalyst 2900XL e 3500XL non supportano SPAN solo in direzione Rx (Rx SPAN o Ingress SPAN) o solo in direzione Tx (Tx SPAN o Ingress SPAN). Tutte le porte SPAN sono progettate per acquisire il traffico in entrambe le direzioni.

---

## SPAN sui Catalyst 2948G-L3 e 4908G-L3

I Catalyst 2948G-L3 e Catalyst 4908G-L3 sono switch-router a configurazione fissa ovvero switch di layer 3. Su uno switch di layer 3, la funzione SPAN è chiamata snooping.

Tuttavia, lo snooping non è supportato su questi switch. Fare riferimento alla sezione [Funzionalità non supportate delle Note sulla versione dei Catalyst 2948G-L3 e Catalyst 4908G-L3 con Cisco IOS Release 12.0\(10\)W5\(18g\)](#).

## SPAN sui Catalyst 8500

Sui Catalyst 8540 è disponibile una funzione SPAN base chiamata snooping delle porte. Per ulteriori informazioni, fare riferimento alla documentazione aggiornata del Catalyst 8540.

Lo snooping delle porte permette di eseguire un mirroring trasparente del traffico proveniente da una o più porte di origine e destinate a un'unica porta di destinazione.

Per configurare il mirroring del traffico basato sulle porte, o snooping, usare il comando snoop. Per disabilitare lo snooping, usare la versione no del comando:

```
<#root>
```

```
snoop interface source_port direction snoop_direction
```

```
no snoop interface source_port
```

La variabile `source_port` fa riferimento alla porta monitorata. La variabile `snoop_direction` è la direzione del traffico sulla porta o sulle porte di origine monitorate: `receive`, `transmission` o `entrambi`.

```
<#root>
```

```
8500CSR#
```

```
configure terminal
```

```
8500CSR(config)#
```

```
interface fastethernet 12/0/15
```

```
8500CSR(config-if)#
```

```
shutdown
```

```
8500CSR(config-if)#
```

```
snoop interface fastethernet 0/0/1 direction both
```

```
8500CSR(config-if)#
```

```
no shutdown
```

L'esempio mostra l'output del comando `show snoop`:


```
<#root>
```

```
8500CSR#
```

```
show snoop
```

```
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option:          (configured=enabled)(actual=enabled)
Snoop direction:      (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

---

 Nota: questo comando non è supportato sulle porte Ethernet in Catalyst 8540 se si esegue un'immagine MSR (Multiservice ATM Switch Router), ad esempio 8540m-in-mz. Usare quindi un'immagine CSR (Campus Switch Router), ad esempio 8540c-in-mz.

---

# SPAN sui Catalyst serie 2900, 4500/4000, 5500/5000 e 6500/6000 Switch con CatOS

Il contenuto di questa sezione è valido esclusivamente per i Cisco Catalyst serie 2900 Switch menzionati di seguito:

- Cisco Catalyst 2948G-L2 Switch
- Cisco Catalyst 2948G-GE-TX Switch
- Cisco Catalyst 2980G-A Switch

Il contenuto di questa sezione è valido esclusivamente per i Cisco Catalyst serie 4000 Switch menzionati di seguito:

- Switch con chassis modulare:
  - Cisco Catalyst 4003 Switch
  - Cisco Catalyst 4006 Switch
- Switch con chassis fisso:
  - Cisco Catalyst 4912G Switch

## SPAN locale

Le funzioni SPAN sono state aggiunte a CatOS singolarmente e raggruppate in un unico comando, `set span`, con cui è possibile configurare lo SPAN. Il comando può essere specificato in dettaglio con numerose opzioni:

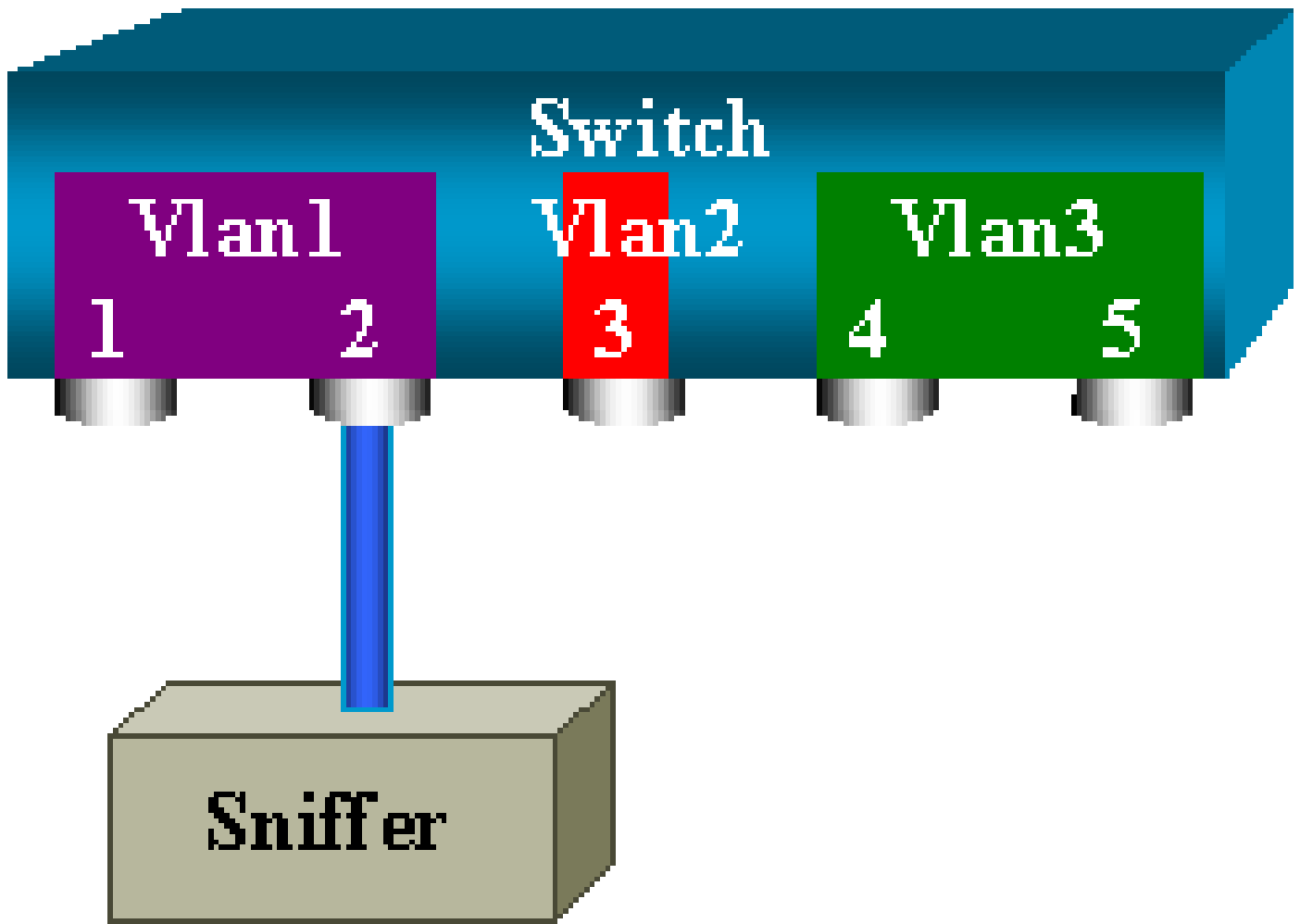
```
<#root>
```

```
switch (enable)
```

```
set span
```

```
Usage: set span disable [dest_mod/dest_port|all]
       set span <src_mod/src_ports...|src_vlans...|sc0>
           <dest_mod/dest_port> [rx|tx|both]
           [inpkts <enable|disable>]
           [learning <enable|disable>]
           [multicast <enable|disable>]
           [filter <vlans...>]
           [create]
```

Questo esempio di rete illustra le diverse possibilità dello SPAN quando si usano le opzioni:



Nello schema è rappresentata una parte di una scheda di linea, installata nello slot 6 di uno switch Catalyst 6500/6000. In questo scenario:

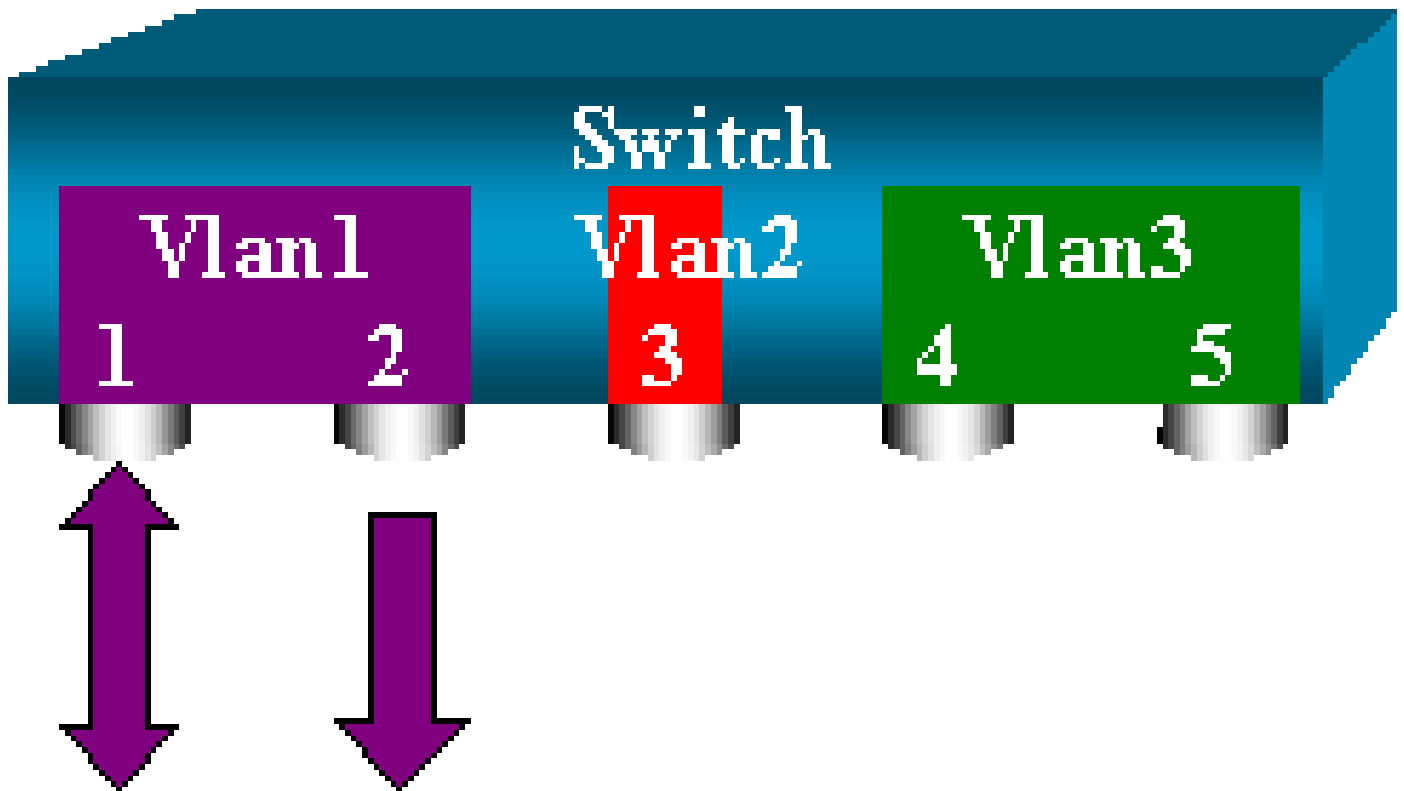
- Le porte 6/1 e 6/2 appartengono alla VLAN 1
- La porta 6/3 appartiene alla VLAN 2
- Le porte 6/4 e 6/5 appartengono alla VLAN 3

Collegare uno sniffer alla porta 6/2 e usarlo come porta di monitoraggio nei diversi scenari.

PSPAN, VSPAN: monitorare alcune porte o un'intera VLAN

Per monitorare una sola porta, usare la versione base del comando set span. La sintassi è set span source\_port destination\_port.

Monitoraggio di una porta con lo SPAN



```
<#root>
```

```
switch (enable)
```

```
set span 6/1 6/2
```

```
Destination : Port 6/2
```

```
Admin Source : Port 6/1
```

```
Oper Source : Port 6/1
```

```
Direction : transmit/receive
```

```
Incoming Packets: disabled
```

```
Learning : enabled
```

```
Multicast : enabled
```

```
Filter : -
```

```
Status : active
```

```
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
```

```
session active for destination port 6/2
```

Con questa configurazione, ogni pacchetto ricevuto o inviato dalla porta 6/1 viene copiato sulla porta 6/2. Una descrizione chiara di ciò viene visualizzata quando si immette la configurazione. Usare il comando `show span` per visualizzare un riepilogo della configurazione SPAN corrente:

```
<#root>
```

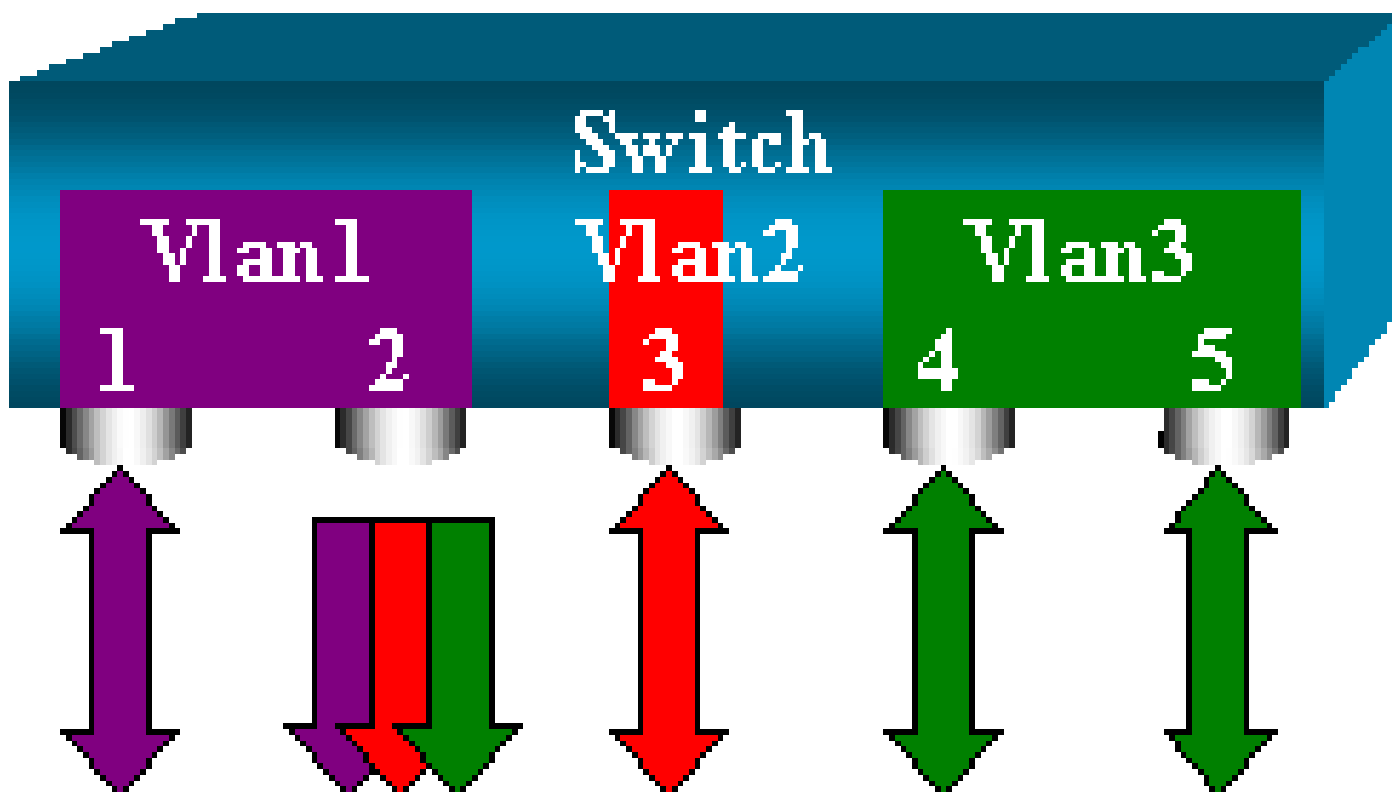
```
switch (enable)
```

```
show span
```

Destination : Port 6/2  
Admin Source : Port 6/1  
Oper Source : Port 6/1  
Direction : transmit/receive  
Incoming Packets: disabled  
Learning : enabled  
Multicast : enabled  
Filter : -  
Status : active

Total local span sessions: 1

Monitoraggio di più porte con lo SPAN




Il comando `set span source_ports destination_port` permette all'utente di specificare più porte di origine. È sufficiente elencare tutte le porte su cui si desidera implementare lo SPAN, separate da virgole.

L'interprete della riga di comando permette di usare anche il trattino per specificare un intervallo di porte.

L'esempio mostra come specificare più porte. Nell'esempio lo SPAN viene usato sulla porta 6/1 e su un intervallo di tre porte, da 6/3 a 6/5.

---


 Nota: può esistere una sola porta di destinazione. Specificare sempre la porta di destinazione dopo la porta SPAN di origine.

---

```
switch (enable)
```

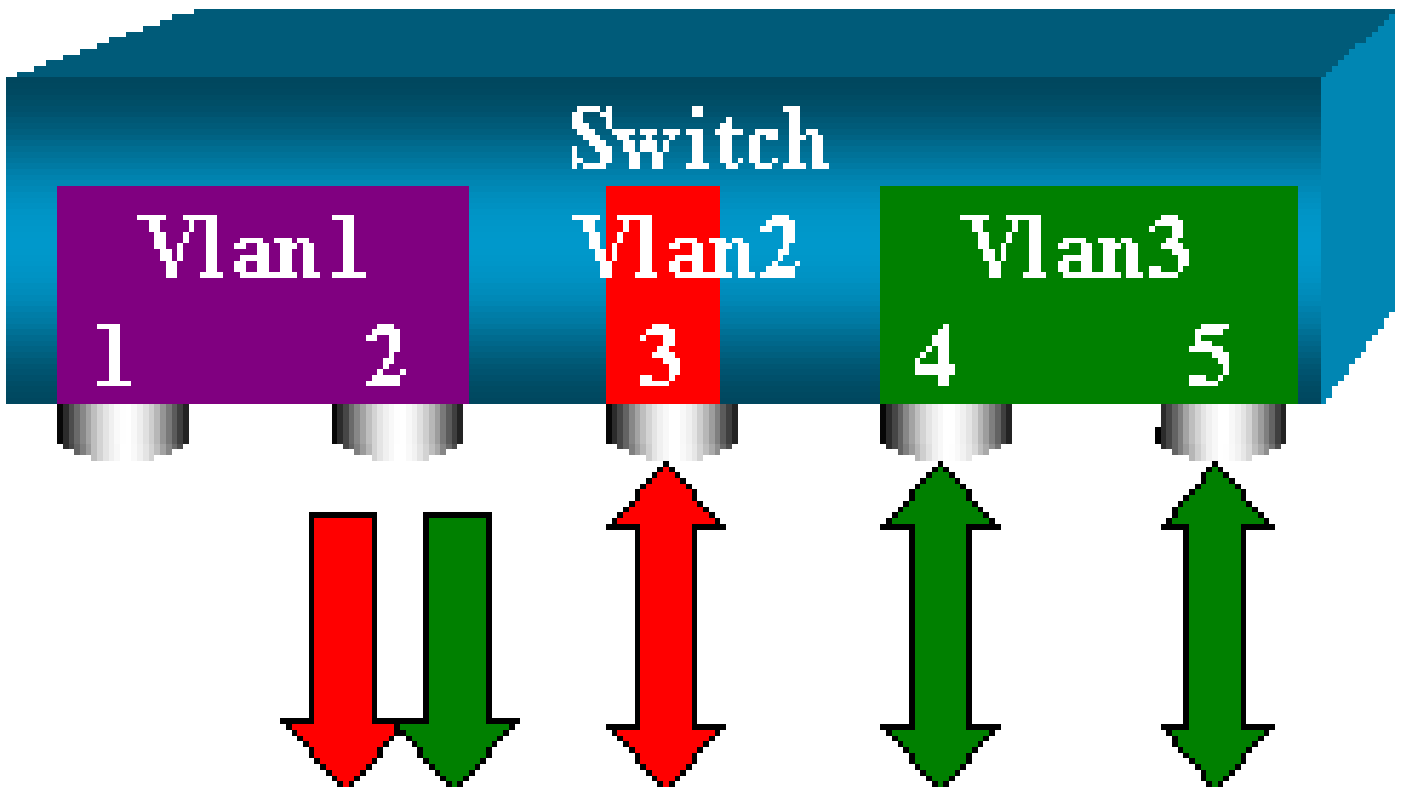
```
set span 6/1,6/3-5 6/2
```

```
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1,6/3-5
Oper Source : Port 6/1,6/3-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

 Nota: a differenza degli switch Catalyst 2900XL/3500XL, gli switch Catalyst 4500/4000, 5500/5000 e 6500/6000 possono monitorare le porte che appartengono a più VLAN diverse con versioni CatOS precedenti alla 5.1. In questo caso, le porte con mirroring vengono assegnate alle VLAN 1, 2 e 3.

### Monitoraggio delle VLAN con lo SPAN

Infine, il comando `set span` permette di configurare una porta su cui monitorare il traffico locale di un'intera VLAN. Il comando è `set span source_vlan(s) destination_port`.





Usare un elenco di una o più VLAN come origine, anziché un elenco di porte:

```
<#root>
```


```
switch (enable)
```

```
set span 2,3 6/2
```

```
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

In questa configurazione, ciascun pacchetto ricevuto o inviato dalla VLAN 2 o 3 viene copiato sulla porta 6/2.

---

 Nota: il risultato è esattamente lo stesso di se si implementa SPAN singolarmente su tutte le porte che appartengono alle VLAN specificate dal comando. Confrontare il campo `Oper Source` (Origine operativa) con il campo `Admin Source` (Origine amministrativa). Il campo `Admin Source` (Origine amministrativa) elenca tutte le porte configurate per la sessione SPAN, il campo `Oper Source` (Origine operativa) elenca tutte le porte che usano lo SPAN.

---

## SPAN in ingresso/in uscita

Nell'esempio illustrato nella sezione [Monitoraggio delle VLAN con lo SPAN](#), viene monitorato il traffico in ingresso e in uscita sulle porte specificate.

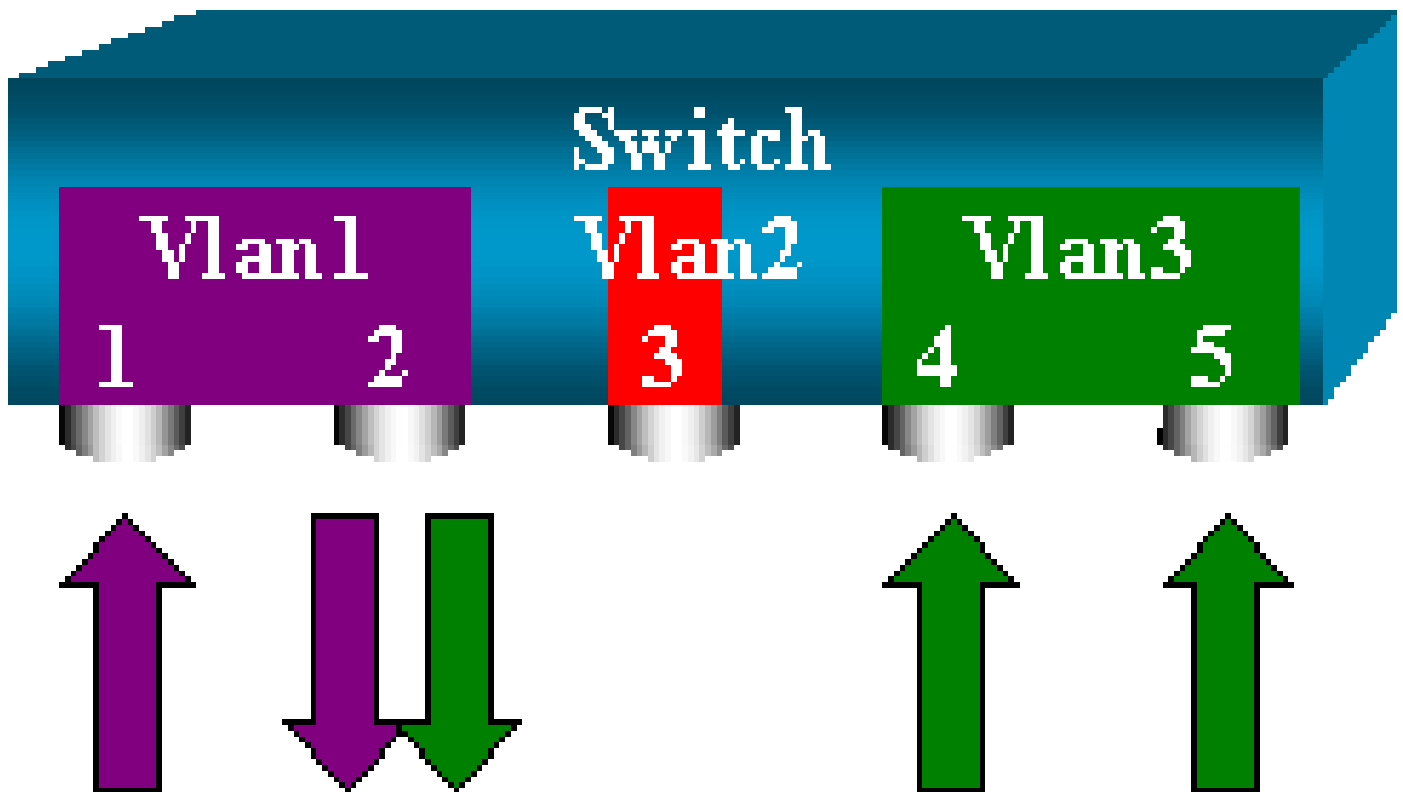
Il campo `Direzione: trasmissione/ricezione` visualizza questa condizione. Sui Catalyst serie 4500/4000, 5500/5000 e 6500/6000 Switch è possibile monitorare solo il traffico in uscita (inviato) o solo il traffico in ingresso (ricevuto) su una determinata porta.

Aggiungere la parola chiave `rx` (ricezione) o `tx` (trasmissione) alla fine del comando. Il valore predefinito è `both` (entrambe le direzioni).

```
<#root>
```

```
set span source_port destination_port [rx | tx | both]
```

Nell'esempio, la sessione acquisisce tutto il traffico in arrivo sulle VLAN 1 e 3 e copia il traffico rilevato sulla porta 6/2:



```
<#root>
```

```
switch (enable)
```

```
set span 1,3 6/2 rx
```

```
2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 1,3
Oper Source : Port 1/1,6/1,6/4-5,15/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

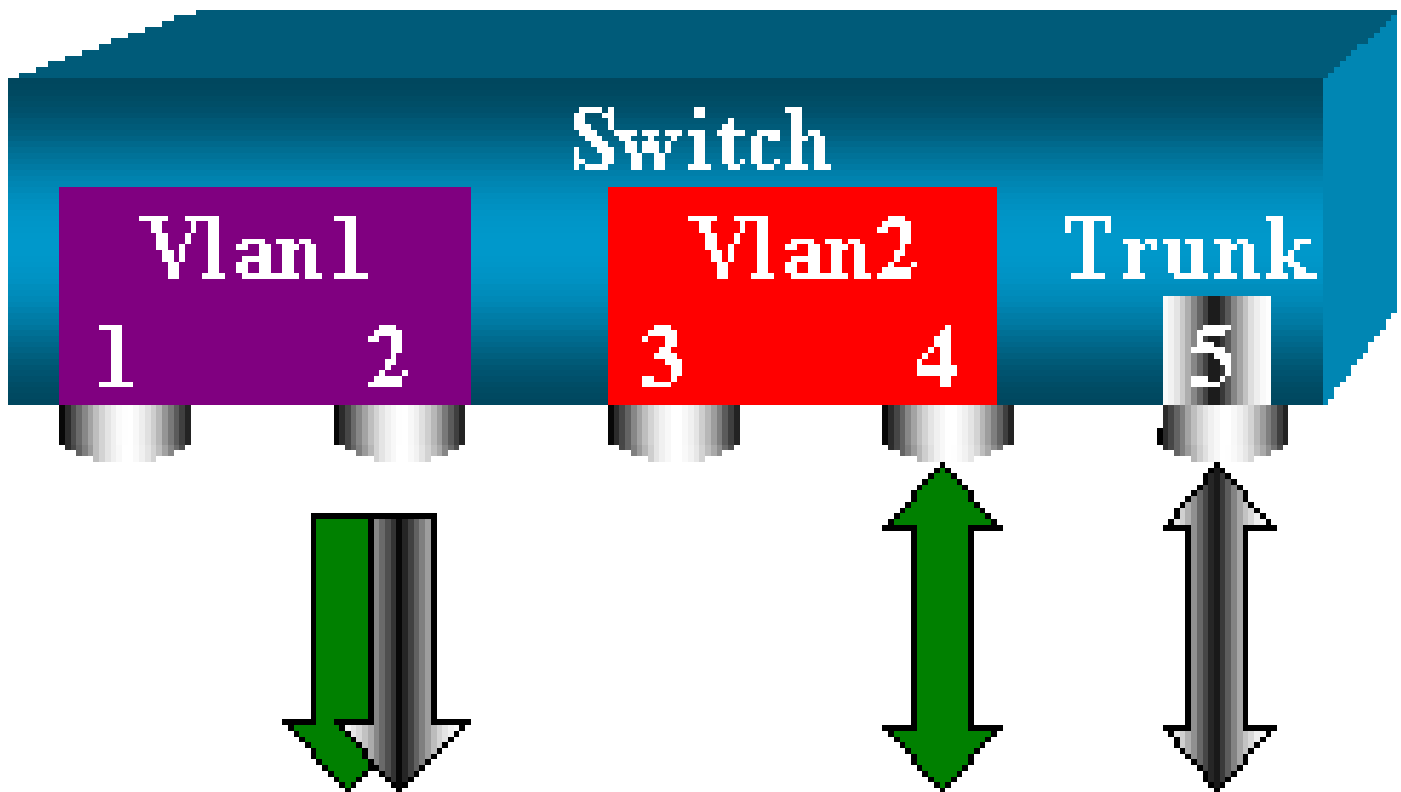
### Implementazione dello SPAN su un trunk

In uno switch, i trunk sono porte speciali in grado di trasportare diverse VLAN. Se si seleziona un trunk come porta di origine, verrà monitorato il traffico di tutte le VLAN del trunk.

## Monitoraggio di un sottogruppo di VLAN appartenenti a un trunk

In questo schema, la porta 6/5 è un trunk su cui passano tutte le VLAN. Si supponga di voler utilizzare lo SPAN sul traffico della VLAN 2 per le porte 6/4 e 6/5. Immettere il comando:

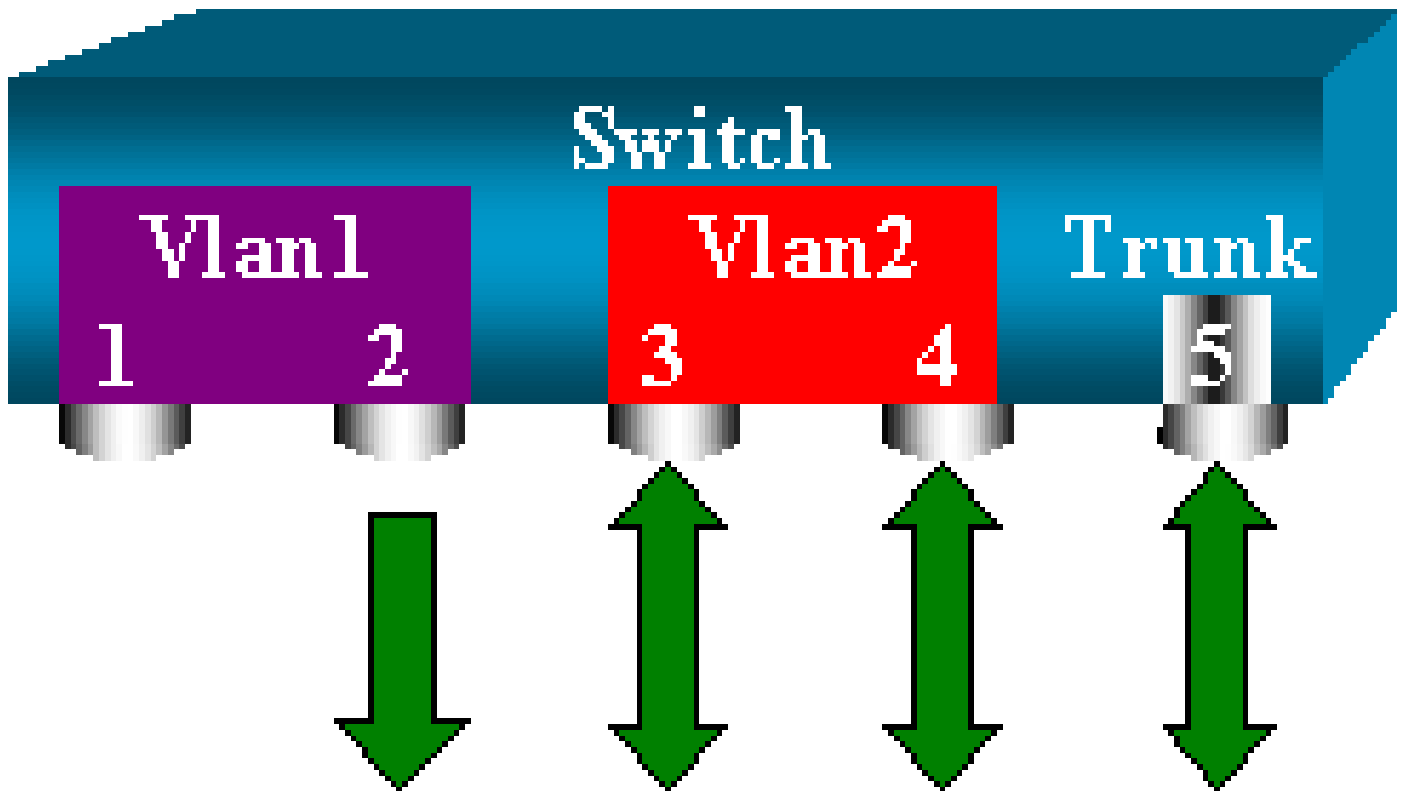
```
<#root>  
switch (enable)  
set span 6/4-5 6/2
```



In questo caso, il traffico ricevuto sulla porta SPAN è una combinazione del traffico desiderato e di tutte le VLAN trasportate dal trunk 6/5.

Ad esempio, non è possibile distinguere sulla porta di destinazione se un pacchetto proviene dalla porta 6/4 nella VLAN 2 o dalla porta 6/5 nella VLAN 1. In alternativa, è possibile usare lo SPAN sull'intera VLAN 2:

```
<#root>  
switch (enable)  
set span 2 6/2
```



In questa configurazione, viene monitorato solo il traffico del trunk che appartiene alla VLAN 2. Il problema è che ora si riceve anche il traffico che non si desiderava dalla porta 6/3.

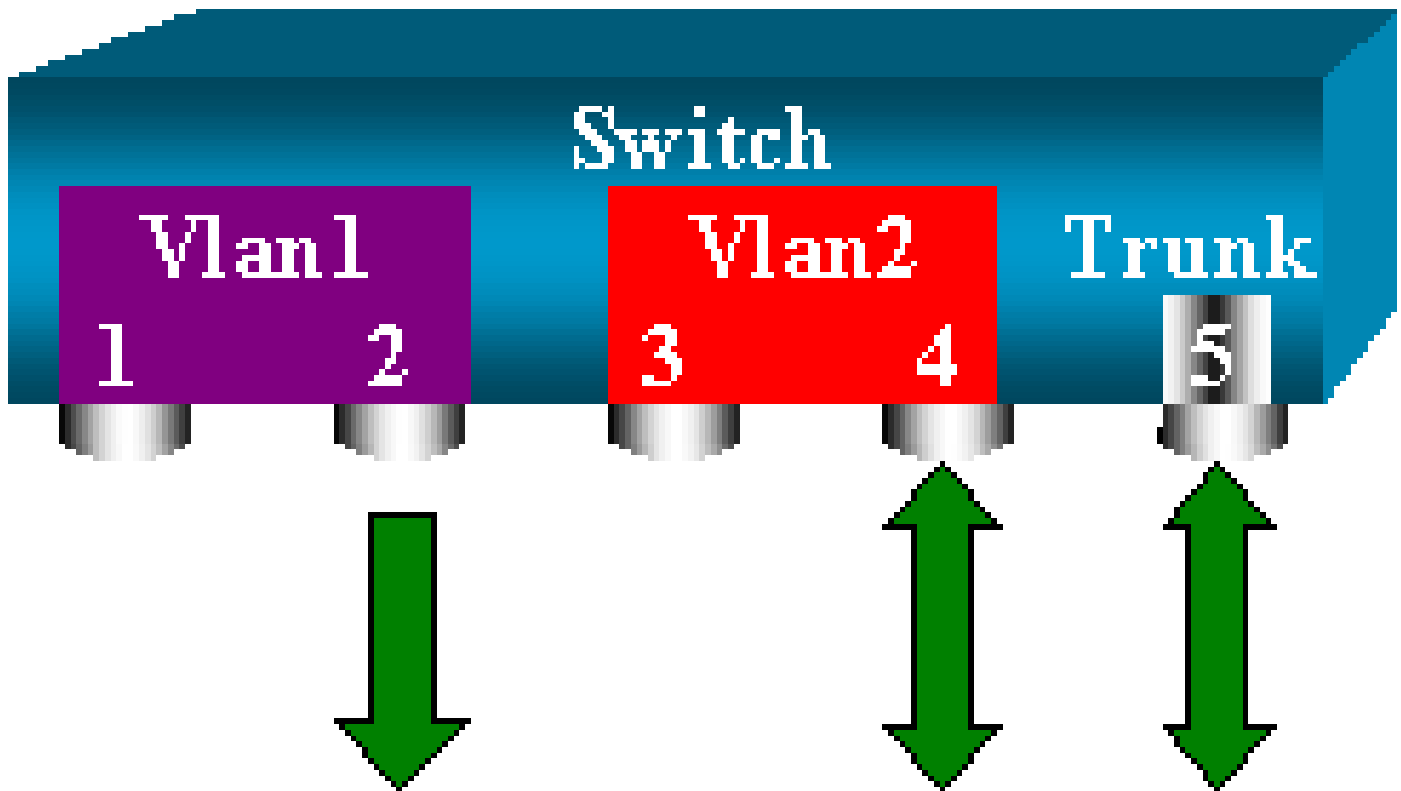
CatOS include un'altra parola chiave che consente di selezionare alcune VLAN da monitorare da un trunk:

```
<#root>
```


```
switch (enable)
```

```
set span 6/4-5 6/2 filter 2
```

```
2000 Sep 06 02:31:51 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
  for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : 2
Status : active
```



Questo comando raggiunge lo scopo, perché seleziona la VLAN 2 su tutti i trunk monitorati. Con questo filtro è possibile specificare diverse VLAN.

 Nota: questa opzione filtro è supportata solo sugli switch Catalyst 4500/4000 e Catalyst 6500/6000. I Catalyst 5500/5000 non supportano questo filtro, disponibile nel comando `set span`.

### Trunking sulla porta di destinazione

Se le porte di origine appartengono a VLAN diverse, o se si usa la funzione SPAN su più VLAN di una porta trunk, potrebbe essere necessario sapere a quale VLAN appartiene il pacchetto ricevuto sulla porta SPAN di destinazione.

A tal fine, è possibile abilitare il trunking sulla porta di destinazione prima di configurare la porta dello SPAN. In questo modo, tutti i pacchetti inoltrati allo sniffer vengono contrassegnati con i rispettivi ID VLAN.

 Nota: lo sniffer deve riconoscere l'incapsulamento corrispondente.

```
<#root>
```

```
switch (enable)
```

```
set span disable 6/2
```

This command will disable your span session.

```
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/4-5
2000 Sep 06 02:52:22 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
switch (enable)
```

```
set trunk 6/2 nonegotiate isl
```

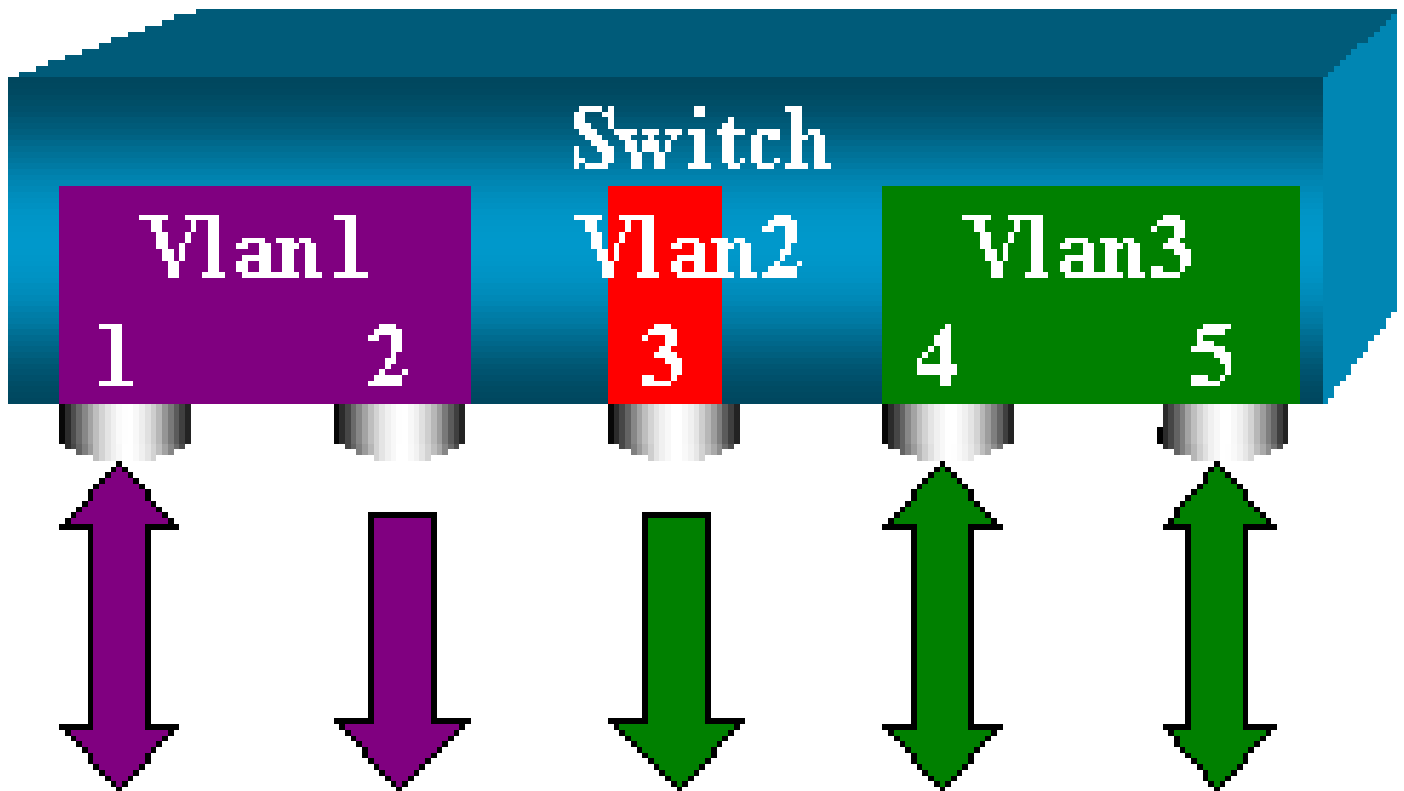
```
Port(s) 6/2 trunk mode set to nonegotiate.
Port(s) 6/2 trunk type set to isl.
switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
isl trunk
switch (enable)
```

```
set span 6/4-5 6/2
```

```
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
2000 Sep 06 02:53:23 %SYS-5-SPAN_CFGSTATECHG:local span session active for
destination port 6/2
```

## Creazione di più sessioni simultanee

Negli esempi mostrati finora è stata creata sempre una sola sessione SPAN. Ogni volta che si usa un nuovo comando set span, la configurazione precedente viene annullata. In CatOs invece si possono eseguire più sessioni contemporaneamente e avere più porte di destinazione allo stesso tempo. Usare il comando set span source destination create per aggiungere un'altra sessione SPAN. In questa sessione, vengono monitorate le porte da 6/1 a 6/2 e, allo stesso tempo, la VLAN 3 sulla porta 6/3:



```
<#root>
```

```
switch (enable)
```

```
set span 6/1 6/2
```

```
2000 Sep 05 08:49:04 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:49:05 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
switch (enable)
```

```
set span 3 6/3 create
```

```
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:55:38 %SYS-5-SPAN_CFGSTATECHG:local span
```

session active for destination port 6/3

Usare ora il comando show span per verificare la presenza delle due sessioni:

```
<#root>
```

```
switch (enable)
```

```
show span
```

```
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
```

```
-----
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
Total local span sessions: 2
```

È possibile così creare altre sessioni. In caso sia necessario invece eliminare una sessione, il comando è:

```
<#root>
```

```
set span disable {all | destination_port}
```

Poiché è possibile avere una sola porta di destinazione per sessione, la porta di destinazione identifica la sessione. Eliminare la prima sessione creata, ossia la sessione che usa la porta 6/2 come destinazione:

```
<#root>
```

```
switch (enable)
```

```
set span disable 6/2
```

This command will disable your span session.



```
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/1
2000 Sep 05 09:04:33 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
```

È ora possibile verificare che sia rimasta una sola sessione:

```
<#root>
```

```
switch (enable)
```

```
show span
```

```
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
```

```
Total local span sessions: 1
```

Per disabilitare tutte le sessioni correnti con un'unica operazione, usare il comando:

```
<#root>
```

```
switch (enable)
```

```
set span disable all
```

```
This command will disable all span session(s).
Do you want to continue (y/n) [n]?y
Disabled all local span sessions
2000 Sep 05 09:07:07 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/3
```

```
switch (enable)
```

```
show span
```

```
No span session configured
```

Altre opzioni SPAN

La sintassi del comando set span è:

<#root>

switch (enable)

set span

Usage: set span disable [dest\_mod/dest\_port|all]  
set span <src\_mod/src\_ports...|src\_vlans...|sc0>  
      <dest\_mod/dest\_port> [rx|tx|both]

[inpmts

]

[learning

]

[multicast

]

[filter <vlans...>]  
[create]

In questa sezione vengono descritte brevemente le opzioni discusse nel documento:

- sc0 - La parola chiave sc0 viene specificata in una configurazione SPAN quando è necessario monitorare il traffico verso l'interfaccia di gestione sc0. Questa funzione è disponibile sugli switch Catalyst 5500/5000 e 6500/6000, versione codice CatOS 5.1 o successiva.
- inpkts enable/disable: un'opzione molto importante. Come spiegato in questo documento, una porta configurata come porta SPAN di destinazione appartiene ancora alla sua VLAN d'origine. I pacchetti ricevuti su una porta di destinazione entrano quindi nella VLAN, come se questa porta fosse una normale porta di accesso. Questo potrebbe essere un comportamento desiderato. Se si usa un PC come sniffer, si potrebbe volere che questo PC sia collegato alla VLAN. Tuttavia, la connessione potrebbe rivelarsi pericolosa, se la porta di destinazione è collegata anche ad altre apparecchiature che creano un loop nella rete. Sulla porta SPAN di destinazione il protocollo SPAN non viene eseguito e potrebbe crearsi una situazione pericolosa di bridging loop. Per informazioni su come questa situazione può verificarsi, vedere la sezione [Perché la sessione SPAN crea un loop di bridging](#) di questo documento. Per impostazione predefinita, questa opzione è disabilitata, quindi la porta SPAN di destinazione ignora i pacchetti ricevuti. Ignorando i pacchetti, il sistema protegge la porta dai bridging loop. L'opzione è disponibile in CatOS dalla versione 4.2.
- learning enable/disable: l'opzione permette di disabilitare l'apprendimento sulla porta di destinazione. Per impostazione predefinita, l'apprendimento è abilitato e la porta di destinazione acquisisce gli indirizzi MAC dei pacchetti in arrivo sulla porta. Questa funzione è disponibile in CatOS 5.2 sui Catalyst 4500/4000 e 5500/5000 e in CatOS 5.3 sui Catalyst 6500/6000.
- multicast enable/disable: come suggerisce il nome, l'opzione permette di abilitare o disabilitare il monitoraggio di pacchetti multicast. Per impostazione predefinita, l'opzione è abilitata. Questa funzione è disponibile sui Catalyst 5500/5000 e 6500/6000 con CatOS 5.1 e versioni successive.
- spanning port 15/1: sui Catalyst 6500/6000, è possibile usare la porta 15/1 (o 16/1) come porta SPAN di origine. Sulla porta è possibile monitorare il traffico inoltrato alla scheda MSFC (Multilayer Switch Feature Card). La porta acquisisce il traffico indirizzato tramite software o diretto alla scheda MSFC.

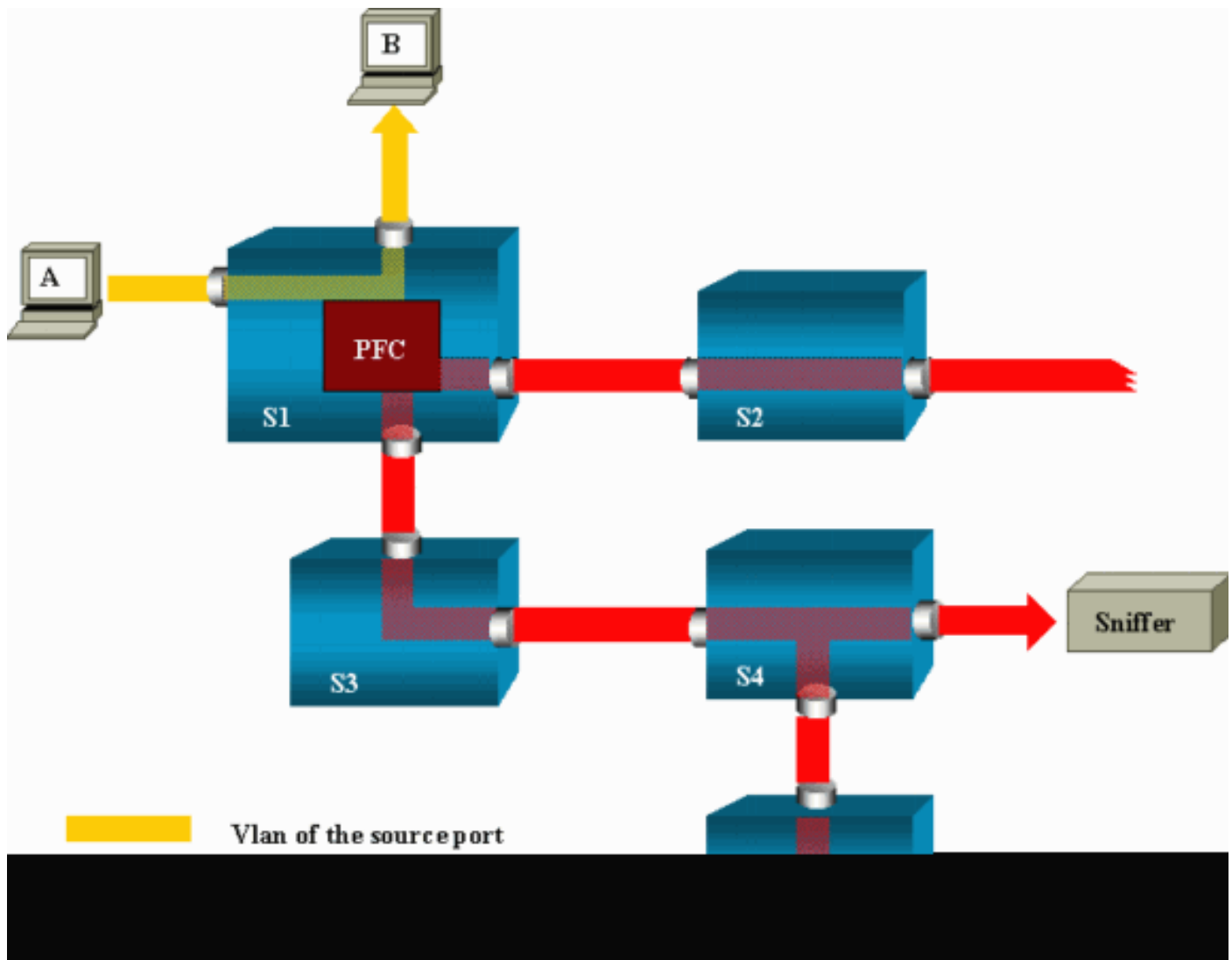
## RSPAN (Remote SPAN)

### Panoramica di RSPAN

Anziché monitorare uno switch solo in locale con la funzione SPAN, la funzione RSPAN permette di monitorare le porte di origine presenti su un'intera rete commutata. La funzionalità è disponibile sui Catalyst serie 6500/6000 Switch con CatOS 5.3 ed è stata aggiunta ai Catalyst serie 4500/4000 Switch con CatOS 6.3 e versioni successive.

La logica di questa funzionalità è uguale a quella di una normale sessione SPAN. Il traffico monitorato dallo SPAN non viene copiato direttamente sulla porta di destinazione, ma inoltrato a tutte le porte di una RSPAN VLAN speciale. La porta di destinazione può quindi trovarsi in qualsiasi punto di questa RSPAN VLAN. Infine, è possibile avere più porte di destinazione.

Nello schema è illustrata la struttura di una sessione RSPAN:



Nell'esempio la funzione RSPAN viene configurata in modo da monitorare il traffico inviato dall'host A. Quando l'host A genera un frame destinato all'host B, il pacchetto viene copiato in una RSPAN VLAN predefinita da un circuito ASIC (Application-Specific Integrated Circuit) presente sulla scheda PFC (Policy Feature Card) del Catalyst 6500/6000. Da lì, il pacchetto viene quindi inviato a tutte le altre porte che appartengono alla RSPAN VLAN. Tutti i collegamenti tra switch delineati nell'esempio sono trunk. Questo è un requisito della funzione RSPAN. Le uniche porte di accesso sono le porte di destinazione, a cui sono collegati gli sniffer (nell'esempio, sugli switch S4 e S5).

Alcune considerazioni su questa configurazione:

- S1 è lo switch di origine. I pacchetti entrano nella RSPAN VLAN solo se gli switch sono configurati come origine RSPAN. Al momento, uno switch può essere solo l'origine di una

sessione RSPAN, quindi uno switch di origine può servire solo una RSPAN VLAN alla volta.

- S2 e S3 sono gli switch intermedi. Non sono origini RSPAN e non hanno porte di destinazione. Uno switch può essere intermedio per un numero qualsiasi di sessioni RSPAN.
- S4 e S5 sono switch di destinazione. Alcune porte sono configurate come destinazione di una sessione RSPAN. Al momento, un Catalyst 6500/6000 può avere fino a 24 porte RSPAN di destinazione, per una o più sessioni diverse. Tenere presente anche che S4 è sia uno switch di destinazione che uno switch intermedio.
- Come si evince dallo schema, i pacchetti RSPAN vengono inoltrati a tutte le porte della RSPAN VLAN. Anche gli switch che non sono sul percorso di una porta di destinazione, ad esempio lo switch S2, ricevono il traffico destinato alla RSPAN VLAN. Può essere quindi utile ridurre la VLAN sui collegamenti S1-S2.
- Per assicurare che i pacchetti vengano inviati a tutte le porte, l'apprendimento sulla RSPAN VLAN è disabilitato.
- Al fine di prevenire eventuali loop, la RSPAN VLAN continua a usare il protocollo STP. Pertanto, l'analizzatore RSPAN non può monitorare le unità BPDU (Bridge Protocol Data Unit).

#### Esempio di configurazione dell'analizzatore RSPAN

In questa sezione viene spiegato come definire i diversi elementi in una configurazione RSPAN molto semplice. S1 e S2 sono due Catalyst 6500/6000. Per monitorare alcune porte S1 o le VLAN dello switch S2, è necessario configurare una RSPAN VLAN dedicata. Il resto dei comandi hanno una sintassi simile a quella usata nelle normali sessioni SPAN.



#### Impostazione del trunk ISL tra i due switch S1 e S2

Per iniziare, specificare lo stesso dominio VLAN Trunk Protocol (VTP) su ciascuno switch e scegliere lo switch su cui impostare il trunking. I restanti passaggi vengono eseguiti tramite negoziazione VTP. Sullo switch S1 usare il comando:

```
<#root>
```

```
S1> (enable)
```

```
set vtp domain cisco
```

```
VTP domain cisco modified
```

Sullo switch S2 usare il comando:

```
<#root>
```

```
S2> (enable)
```

```
set vtp domain cisco
```

```
VTP domain cisco modified
```

```
S2> (enable)
```

```
set trunk 5/1 desirable
```

```
Port(s) 5/1 trunk mode set to desirable.
```

```
S2> (enable) 2000 Sep 12 04:32:44 %PAGP-5-PORTFROMSTP:Port 5/1 left bridge  
port 5/1
```

```
2000 Sep 12 04:32:47 %DTP-5-TRUNKPORTON:Port 5/1 has become isl trunk
```

## Creazione della RSPAN VLAN

Ogni sessione RSPAN richiede una VLAN specifica. Questa VLAN deve essere creata. Non è possibile trasformare una VLAN esistente in una RSPAN VLAN. In questo esempio viene utilizzata la VLAN 100:

```
<#root>
```

```
S2> (enable)
```

```
set vlan 100 rspan
```

```
Vlan 100 configuration successful
```

Usare questo comando su uno switch configurato come server VTP. La creazione della RSPAN VLAN 100 viene resa nota automaticamente all'intero dominio VTP.

Configurazione della porta 5/2 dello switch S2 come porta di destinazione RSPAN

```
<#root>
```

```
S2> (enable)
```

```
set rspan destination 5/2 100
```

```
Rspan Type : Destination
Destination : Port 5/2
Rspan Vlan : 100
Admin Source : -
Oper Source : -
Direction : -
Incoming Packets: disabled
Learning : enabled
Multicast : -
Filter : -
Status : active
2000 Sep 12 04:34:47 %SYS-5-SPAN_CFGSTATECHG:remote span destination session
active for destination port 5/2
```

## Configurazione di una porta di origine RSPAN sullo switch S1

Nell'esempio viene monitorato il traffico ricevuto dallo switch S1 sulla porta 6/2. Immettere questo comando

```
<#root>
```

```
S1> (enable)
```

```
set rspan source 6/2 100 rx
```

```
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
S1> (enable) 2000 Sep 12 05:40:37 %SYS-5-SPAN_CFGSTATECHG:remote span
source session active for remote span vlan 100
```

Tutti i pacchetti in arrivo sulla porta 6/2 vengono ora inoltrati all'intera RSPAN VLAN 100 e viaggiano nel trunk fino a raggiungere la porta di destinazione configurata sullo switch S1.

## Verifica della configurazione

Per visualizzare un riepilogo della configurazione RSPAN corrente dello switch, usare il comando show rspan. Anche in questo scenario, è possibile avere una sola sessione RSPAN di origine alla

volta.

<#root>

S1> (enable)

show rspan

```
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
Total remote span sessions: 1
```

Altre configurazioni possibili con il comando set rspan

Quando si usa RSPAN, la configurazione delle porte di origine e di destinazione occupa diverse righe di comando. A parte questa differenza, le funzioni SPAN e RSPAN hanno la stessa logica di funzionamento. Per avere più porte SPAN di destinazione, è possibile usare la funzione RSPAN in locale, su un unico switch.

## Riepilogo delle funzioni e limitazioni

In questa tabella vengono riepilogate le diverse funzioni introdotte. Inoltre, viene indicata la versione CatOS minima per eseguire ciascuna funzione sulla piattaforma specifica:

Funzionalità	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
Opzione inpkts enable/disable	4.4	4.2	5.1
Più sessioni, porte in VLAN diverse	5.1	5.1	5.1
Opzione sc0	—	5.1	5.1
Opzione multicast enable/disable	—	5.1	5.1
Opzione learning enable/disable	5.2	5.2	5.3
RSPAN	6.3	—	5.3

In questa tabella viene fornito un breve riepilogo delle limitazioni al momento valide per il numero di sessioni SPAN ammesse:

Funzionalità	Catalyst serie 4500/4000 Switch	Catalyst serie 5500/5000 Switch	Catalyst serie 6500/6000 Switch
--------------	---------------------------------------	---------------------------------------	------------------------------------



Sessioni SPAN in ricezione o in entrambe le direzioni	5	1	2
Sessioni SPAN in trasmissione	5	4	4
Sessioni Mini Protocol Analyzer	Non supportata	Non supportata	1
Sessioni RSPAN di origine in ricezione, in trasmissione o in entrambe le direzioni	5	Non supportata	1 Supervisor Engine 720 supporta due sessioni RSPAN di origine.
Destinazione RSPAN	5	Non supportata	24
Totale sessioni	5	5	30

Per ulteriori informazioni sulle limitazioni e le linee guida per la configurazione, fare riferimento ai seguenti documenti:

- [Configurazione di SPAN e RSPAN](#) (Catalyst 4500/4000)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 6500/6000)

## SPAN sui Catalyst serie 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E Switch

Di seguito vengono fornite linee guida per la configurazione della funzione SPAN sui Catalyst serie 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E Switch:

- I Catalyst 2950 Switch possono avere solo una sessione SPAN attiva alla volta e possono monitorare solo le porte di origine. Questi switch non possono monitorare le VLAN.
- I Catalyst 2950 e 3550 Switch possono inoltrare il traffico a una porta SPAN di destinazione in Cisco IOS Software Release 12.1(13)EA1 e versioni successive.
- I Catalyst 3550, 3560 e 3750 Switch possono supportare fino a due sessioni SPAN alla volta e possono monitorare sia le porte di origine sia le VLAN.
- Sui Catalyst 2970, 3560 e 3750 Switch non è necessario configurare una porta reflector quando si configura una sessione RSPAN.
- Sui Catalyst 3750 Switch è possibile configurare la sessione usando le porte di origine e di destinazione che si trovano su uno switch qualsiasi dello stack.
- È consentita una sola porta di destinazione per sessione SPAN; la stessa porta non può essere una porta di destinazione per più sessioni SPAN. Pertanto, non è possibile avere due sessioni SPAN che usano la stessa porta di destinazione.

Sui Catalyst 2950 e Catalyst 3550 vengono usati comandi di configurazione simili per la funzione SPAN. Tuttavia, i Catalyst 2950 non possono monitorare le VLAN. Per configurare la funzione SPAN, attenersi a questo esempio:

<#root>

```
C2950#
```

```
configure terminal
```

```
C2950(config)#
```

```
C2950(config)#
```

```
monitor session 1 source interface fastethernet 0/2
```

*!--- This configures interface Fast Ethernet 0/2 as source port.*

```
C2950(config)#
```

```
monitor session 1 destination interface fastethernet 0/3
```

*!--- This configures interface Fast Ethernet 0/3 as destination port.*

```
C2950(config)#
```

```
C2950#
```

```
show monitor session 1
```

```
Session 1-----
```

```
Source Ports:
```

```
  RX Only:      None
```

```
  TX Only:      None
```

```
  Both:         Fa0/2
```

```
Destination Ports: Fa0/3
```

```
C2950#
```

È inoltre possibile configurare una porta di destinazione per le funzioni SPAN e RSPAN locali per lo stesso traffico VLAN. Per monitorare il traffico di una VLAN specifica che risiede in due switch collegati direttamente, usare i seguenti comandi sullo switch in cui si trova la porta di destinazione. Nell'esempio viene monitorato il traffico proveniente dalla VLAN 5 che riguarda due switch:

```
<#root>
```

```
c3750(config)#
```

```
monitor session 1 source vlan < Remote RSPAN VLAN ID >
```

```
c3750(config)#
```

```
monitor session 1 source vlan 5
```

```
c3750(config)#
```

```
monitor session 1 destination interface fastethernet 0/3
```

*!--- This configures interface FastEthernet 0/3 as a destination port.*

Sullo switch remoto, usare questa configurazione:

```
<#root>
```

```
c3750_remote(config)#
```

```
monitor session 1 source vlan 5
```


*!--- Specifies VLAN 5 as the VLAN to be monitored.*

```
c3750_remote(config)#
```


```
monitor session 1 destination remote vlan
```

Nell'esempio precedente una porta è stata configurata come porta di destinazione per lo SPAN e l'RSPAN locali, in modo da monitorare il traffico della stessa VLAN che risiede su due switch.


---

 Nota: a differenza degli switch serie 2900XL e 3500XL, gli switch Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 e 3750-E supportano l'SPAN sul traffico delle porte di origine solo in direzione Rx (Rx SPAN o Ingress SPAN), Solo direzione x (Tx SPAN o SPAN in uscita) o entrambe.


---

 Nota: i comandi nella configurazione non sono supportati su Catalyst 2950 con software Cisco IOS versione 12.0(5.2)WC(1) o su qualsiasi software precedente al software Cisco IOS versione 12.1(6)EA2. Per configurare lo SPAN su uno switch Catalyst 2950 con software precedente a quello di Cisco IOS versione 12.1(6)EA2, consultare la sezione [Abilitazione](#) dello [switch port Analyzer](#) di [Gestione degli switch](#).

---

 Nota: sugli switch Catalyst 2950 con software Cisco IOS versione 12.1(9)EA1d e precedenti versioni nel software Cisco IOS versione 12.1 il supporto dei treni è supportato da SPAN. Tuttavia, tutti i pacchetti visibili sulla porta SPAN di destinazione (collegata allo sniffer o al PC) hanno un tag IEEE 802.1Q, anche se la porta SPAN di origine (porta monitorata) potrebbe non essere una porta trunk 802.1Q. Se lo sniffer o la scheda di rete (NIC) del PC non sa decodificare i pacchetti con tag 802.1Q, il dispositivo potrebbe eliminare i pacchetti o avere difficoltà nel tentativo di decodificarli. La capacità di vedere i frame con tag 802.1Q è importante solo quando la porta SPAN di origine è una porta trunk. In Cisco IOS Software Release 12.1(11)EA1 e versioni successive, è possibile abilitare e disabilitare i tag dei pacchetti sulla porta SPAN di destinazione. Per abilitare l'incapsulamento dei pacchetti sulla porta di destinazione, immettere il comando [monitor session session\\_number destination](#)

---

 [interface interface id encapsulation dot1q](#). Se non si specifica la parola chiave encapsulation, i pacchetti vengono inviati senza tag. Questa è anche l'impostazione predefinita in Cisco IOS Software Release 12.1(11)EA1 e versioni successive.

Funzionalità	Catalyst 2950/3550
Opzione inpkts enable/disable (in ingresso)	Cisco IOS Software Release 12.1(12c)EA1
RSPAN	Cisco IOS Software Release 12.1(12c)EA1

Funzionalità	Catalyst 2940 <sup>1</sup> , 2950, 2955, 2960, 2970, 3550, 3560, 3750
Sessioni SPAN in ricezione o in entrambe le direzioni	2
Sessioni SPAN in trasmissione	2
Sessioni RSPAN di origine in ricezione, in trasmissione o in entrambe le direzioni	2
Destinazione RSPAN	2
Totale sessioni	2

<sup>1</sup> I Catalyst 2940 Switch supportano solo la funzione SPAN locale. Su questa piattaforma, la funzione RSPAN non è supportata.

Per ulteriori informazioni sulla configurazione delle funzioni SPAN e RSPAN, fare riferimento alle seguenti guide alla configurazione:

- [Configurazione dello SPAN](#) (Catalyst 2940)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 2950 e 2955)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 2960)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 3550)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 3560)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 3560-E e 3750-E)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 3750)

## SPAN sui Catalyst serie 4500/4000 e Catalyst serie 6500/6000 Switch con software di sistema Cisco IOS

La funzione SPAN è supportata sui Catalyst serie 4500/4000 e sui Catalyst serie 6500/6000 con software di sistema Cisco IOS. Entrambe le piattaforme usano la stessa interfaccia a riga di comando (CLI) e una configurazione della funzione SPAN simile a quanto illustrato nella sezione [SPAN sui Catalyst serie 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560E, 3750 e 3750E Switch](#). Per la configurazione, fare riferimento ai seguenti documenti:

- [Configurazione di SPAN e RSPAN](#) (Catalyst 6500/6000)
- [Configurazione di SPAN e RSPAN](#) (Catalyst 4500/4000)

## Esempio di configurazione

Per configurare la funzione SPAN, attenersi a questo esempio:

```
<#root>
```

```
4507R#
```

```
configure terminal
```

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

```
4507R(config)#
```

```
monitor session 1 source interface fastethernet 4/2
```

*!--- This configures interface Fast Ethernet 4/2 as source port.*

```
4507R(config)#
```

```
monitor session 1 destination interface fastethernet 4/3
```

*!--- The configures interface Fast Ethernet 0/3 as destination port.*

```
4507R#
```

```
show monitor session 1
```

```
Session 1-----
```

```
Type : Local Session
```

```
Source Ports :
```

```
Both : Fa4/2
```

```
Destination Ports : Fa4/3
```

```
4507R#
```


## Riepilogo delle funzioni e limitazioni

In questa tabella vengono riepilogate le diverse funzioni introdotte. Inoltre, viene indicata la versione minima del software Cisco IOS per eseguire ciascuna funzione sulla piattaforma specifica:

Funzionalità	Catalyst 4500/4000 (Cisco IOS Software)	Catalyst 6500/6000 (Cisco IOS Software)
--------------	---	---

Opzione inpkts enable/disable (in ingresso)	Cisco IOS Software Release 12.1(19)EW	Non supportata al momento <sup>1</sup>
RSPAN	Cisco IOS Software Release 12.1(20)EW	Software Cisco IOS Release 12.1(13)E

<sup>1</sup> La funzione non è al momento disponibile. La disponibilità di tali funzioni in genere non viene annunciata fino al rilascio.

 Nota: la funzione SPAN dei Cisco Catalyst serie 6500/6000 Switch ha una limitazione per quanto riguarda il protocollo PIM. Quando si configura uno switch per PIM e SPAN, l'analizzatore di rete o lo sniffer associato alla porta SPAN di destinazione può vedere i pacchetti PIM che non fanno parte del traffico della porta SPAN di origine o della VLAN. Questo problema è causato da una limitazione nella logica di inoltro dei pacchetti dello switch. La porta SPAN di destinazione non esegue alcun controllo per verificare l'origine dei pacchetti. Il problema è documentato dall'ID bug Cisco [CSCdy57506](#) (solo utenti registrati).

In questa tabella viene fornito un breve riepilogo delle limitazioni al momento valide sul numero di sessioni SPAN e RSPAN ammesse:

Funzionalità	Catalyst 4500/4000 (Cisco IOS Software)
Sessioni SPAN in ricezione o in entrambe le direzioni	2
Sessioni SPAN in trasmissione	4
Sessioni RSPAN di origine in ricezione, in trasmissione o in entrambe le direzioni	2 (in ricezione, in trasmissione o in entrambe le direzioni) e fino a 4 solo in trasmissione
Destinazione RSPAN	2
Totale sessioni	6

Sui Catalyst 6500/6000 Switch con software Cisco IOS, fare riferimento a [Limitazioni delle sessioni SPAN, RSPAN ed ERSPAN locali](#).

Sui Catalyst serie 6500 Switch, è importante notare che la funzione SPAN in uscita viene eseguita sul supervisor. In questo modo tutto il traffico soggetto alla funzione SPAN deve essere inviato sul fabric al supervisor e quindi alla porta SPAN di destinazione. Ciò può comportare un significativo uso delle risorse di sistema e influire sul traffico. La funzione SPAN in ingresso viene eseguita sui moduli di ingresso, quindi le sue prestazioni risentiranno delle prestazioni di tutti i motori di replica presenti. Le prestazioni della funzione SPAN dipendono dalle dimensioni del pacchetto e dal tipo di ASIC disponibile nel motore di replica.

Nelle versioni precedenti a Cisco IOS Software Release 12.2(33)SXH, la porta SPAN di destinazione non può essere un'interfaccia port-channel o un EtherChannel. In Cisco IOS Software Release 12.2(33)SXH e versioni successive, un EtherChannel può essere una porta SPAN di destinazione. EtherChannel di destinazione non supporta il protocollo PAgP (Port Aggregation Control Protocol) o il protocollo LACP (Link Aggregation Control Protocol) EtherChannel. È supportata solo la modalità on, con tutto il supporto del protocollo EtherChannel

disabilitato.

Per ulteriori informazioni sulle limitazioni e le linee guida per la configurazione, fare riferimento ai seguenti documenti:

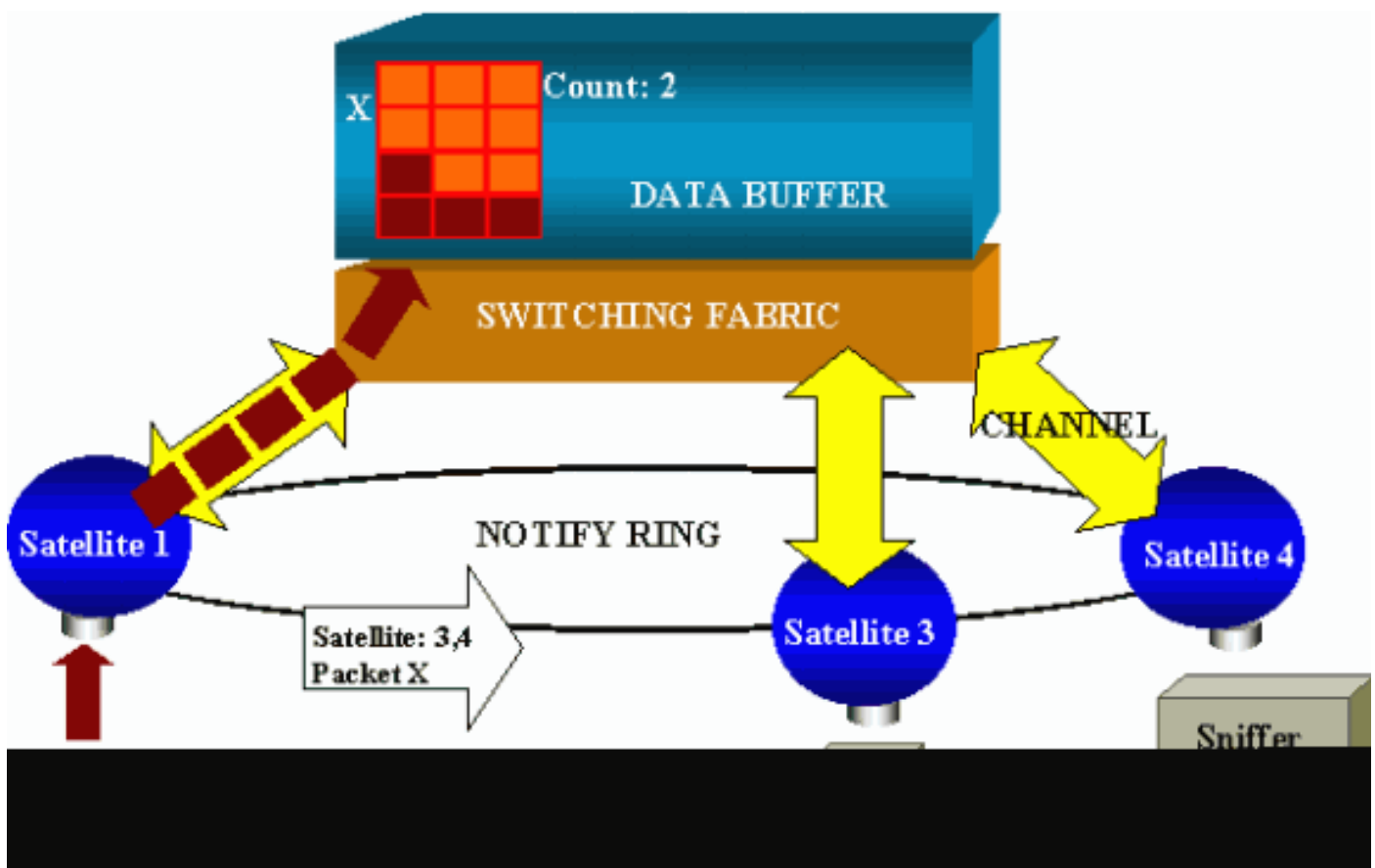
- [Configurazione di SPAN e RSPAN \(Catalyst 4500/4000\)](#)
- [Configurazione di SPAN, Remote SPAN \(RSPAN\) e Encapsulated RSPAN locali \(Catalyst 6500/6000\)](#)

## Conseguenze sulle prestazioni dello SPAN sulle diverse piattaforme Catalyst

Catalyst serie 2900XL/3500XL

Panoramica dell'architettura

Ecco una vista semplificata dell'architettura interna negli switch 2900XL/3500XL:



Le porte dello switch sono collegate a satelliti che comunicano con un fabric di switching tramite canali radiali. Inoltre, tutti i satelliti sono interconnessi tramite un circuito di notifica ad alta velocità dedicato alla segnalazione del traffico.

Quando un satellite riceve un pacchetto da una porta, il pacchetto viene suddiviso in celle e inviato al fabric di switching su uno o più canali. Il pacchetto viene quindi archiviato nella memoria

condivisa. Ciascun satellite conosce le porte di destinazione. Nel diagramma di questa sezione, il satellite 1 sa che il pacchetto X deve essere ricevuto dai satelliti 3 e 4. Il satellite 1 invia un messaggio agli altri satelliti tramite l'anello di notifica. Quindi, i satelliti 3 e 4 possono iniziare a recuperare le celle dalla memoria condivisa tramite i rispettivi canali radiali e infine inoltrare il pacchetto. Poiché il satellite di origine conosce la destinazione, trasmette anche un indice che specifica il numero di volte in cui il pacchetto viene scaricato dagli altri satelliti. Ogni volta che un satellite recupera il pacchetto dalla memoria condivisa, questo indice viene ridotto. Quando l'indice raggiunge 0, la memoria condivisa può essere liberata.

### Conseguenze sulle prestazioni

Per monitorare alcune porte con la funzione SPAN, occorre copiare un'altra volta il pacchetto che viene trasmesso dal buffer dati a un satellite. Le conseguenze sul fabric di switching ad alta velocità sono trascurabili.

La porta di monitoraggio riceve le copie del traffico trasmesso e ricevuto su tutte le porte monitorate. In questa architettura, un pacchetto inviato a più destinazioni viene archiviato nella memoria finché tutte le copie non sono inoltrate. Se la porta di monitoraggio viene usata per oltre il 50% della sua capacità e per un periodo di tempo prolungato, è probabile che si crei una congestione e che la porta occupi una parte della memoria condivisa. È possibile anche che una o più porte monitorate subiscano un rallentamento.

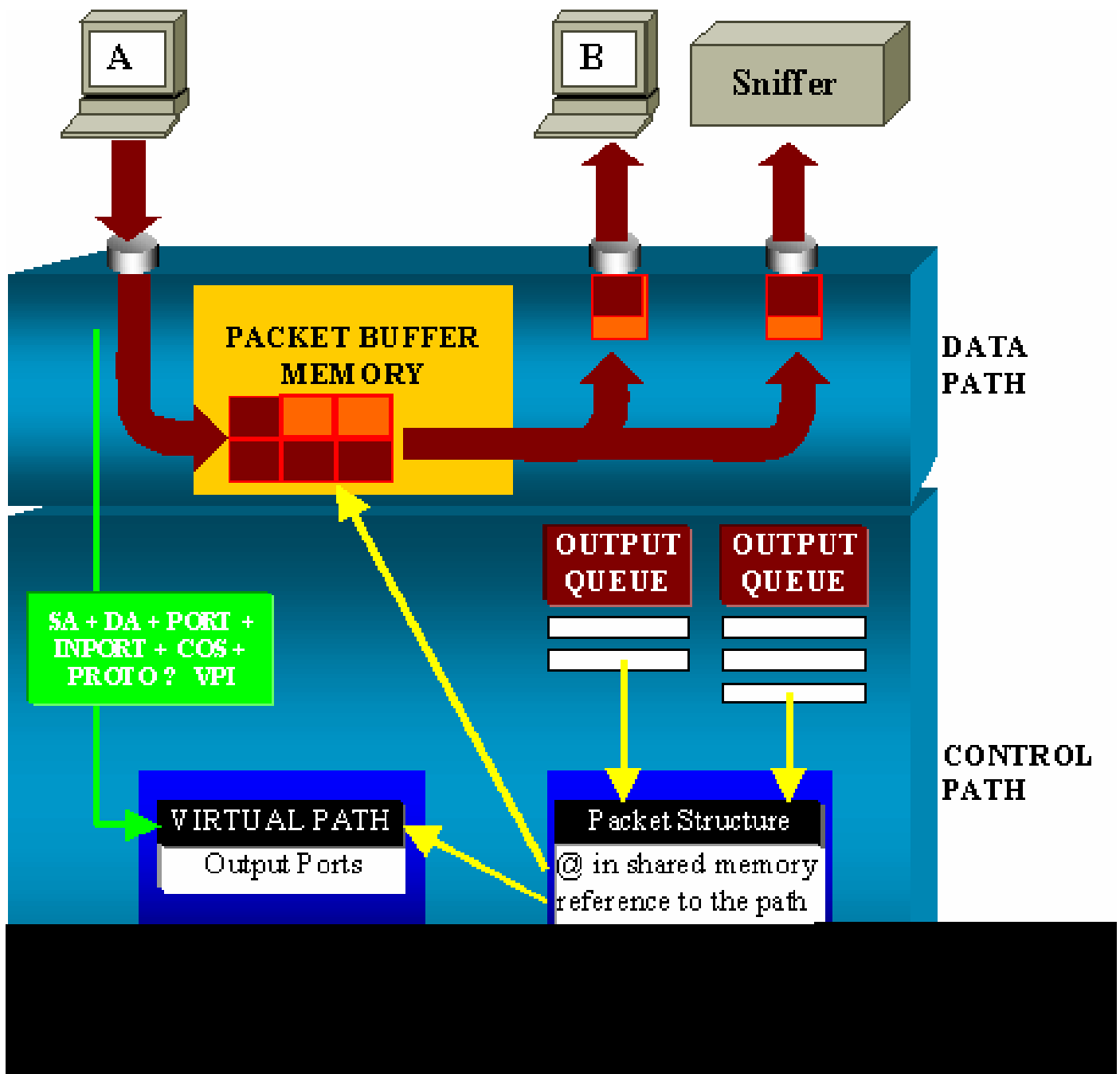
## Catalyst serie 4500/4000

### Panoramica dell'architettura

I Catalyst 4500/4000 si basano su un fabric di switching con memoria condivisa. Questo schema offre una panoramica generale del percorso che il pacchetto segue nello switch.

L'implementazione effettiva è nella pratica molto più complessa:





Sui Catalyst 4500/4000, è possibile distinguere il percorso dei dati. Il percorso dei dati corrisponde al trasferimento effettivo dei dati all'interno dello switch, dal percorso di controllo in cui vengono prese tutte le decisioni.

Quando un pacchetto entra nello switch, viene allocato un buffer nella Packet Buffer Memory, una memoria condivisa.

Una struttura di pacchetti indirizzata a questo buffer viene inizializzata nella tabella dei descrittori PDT (Packet Descriptor Table).

Mentre i dati vengono copiati nella memoria condivisa, il percorso di controllo determina dove effettuare la commutazione del pacchetto. A tal fine, viene calcolato un valore hash sulla base di queste informazioni:

- Indirizzo di origine del pacchetto

- Indirizzo di destinazione
- VLAN
- Tipo di protocollo
- Porta di ingresso
- Classe di servizio (CoS) (tag IEEE 802.1p o impostazione predefinita)

Questo valore viene usato per trovare il Virtual Path Index (VPI) di un percorso nella Virtual Path Table (VPT). Questa voce del percorso virtuale nella VPT contiene diversi campi relativi al flusso specifico.

Le porte di destinazione sono incluse nei campi. La struttura dei pacchetti nella PDT è ora aggiornata con un riferimento al percorso virtuale e al contatore.

Nell'esempio di questa sezione, il pacchetto deve essere trasmesso a due porte diverse, quindi il contatore viene inizializzato su 2. Infine, la struttura del pacchetto viene aggiunta alla coda di output delle due porte di destinazione.

Da lì, i dati vengono copiati dalla memoria condivisa nel buffer di output della porta e il contatore della struttura dei pacchetti diminuisce. Quando raggiunge 0, il buffer della memoria condivisa è vuoto.

#### Conseguenze sulle prestazioni

Quando si usa la funzione SPAN, i pacchetti vengono inviati a due porte diverse, come mostrato nella sezione [Panoramica dell'architettura](#).

L'invio del pacchetto a due porte non costituisce un problema perché il fabric di switching è non bloccante.

Se la porta SPAN di destinazione è congestionata, i pacchetti vengono eliminati nella coda di output e correttamente rimossi dalla memoria condivisa. T

Pertanto, non vi è alcun impatto sul funzionamento dello switch.

## Catalyst serie 5500/5000 e 6500/6000

### Panoramica dell'architettura

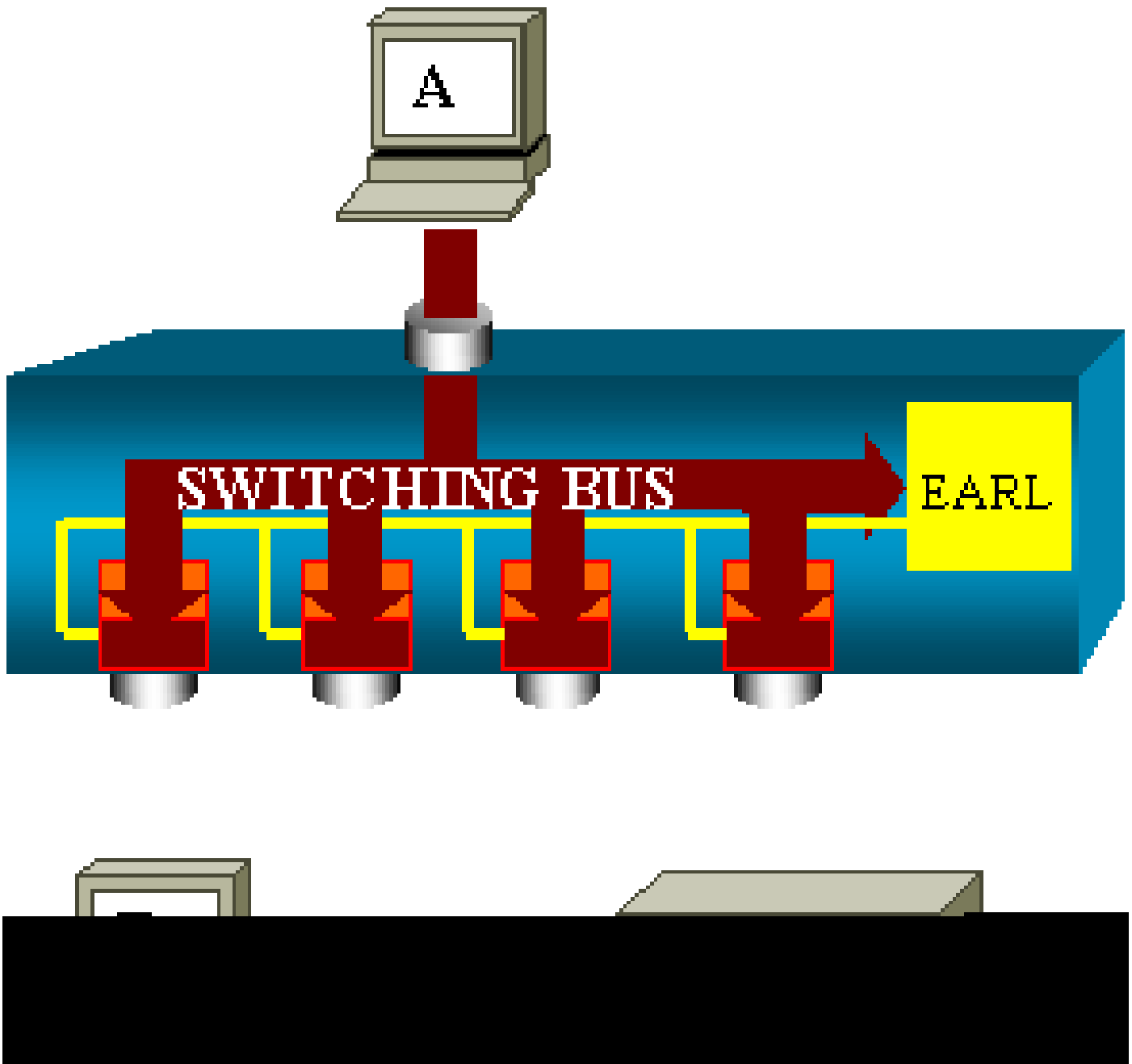
Sui Catalyst serie 5500/5000 e 6500/6000 Switch, i pacchetti ricevuti su una porta vengono trasmessi sul bus di commutazione interno.

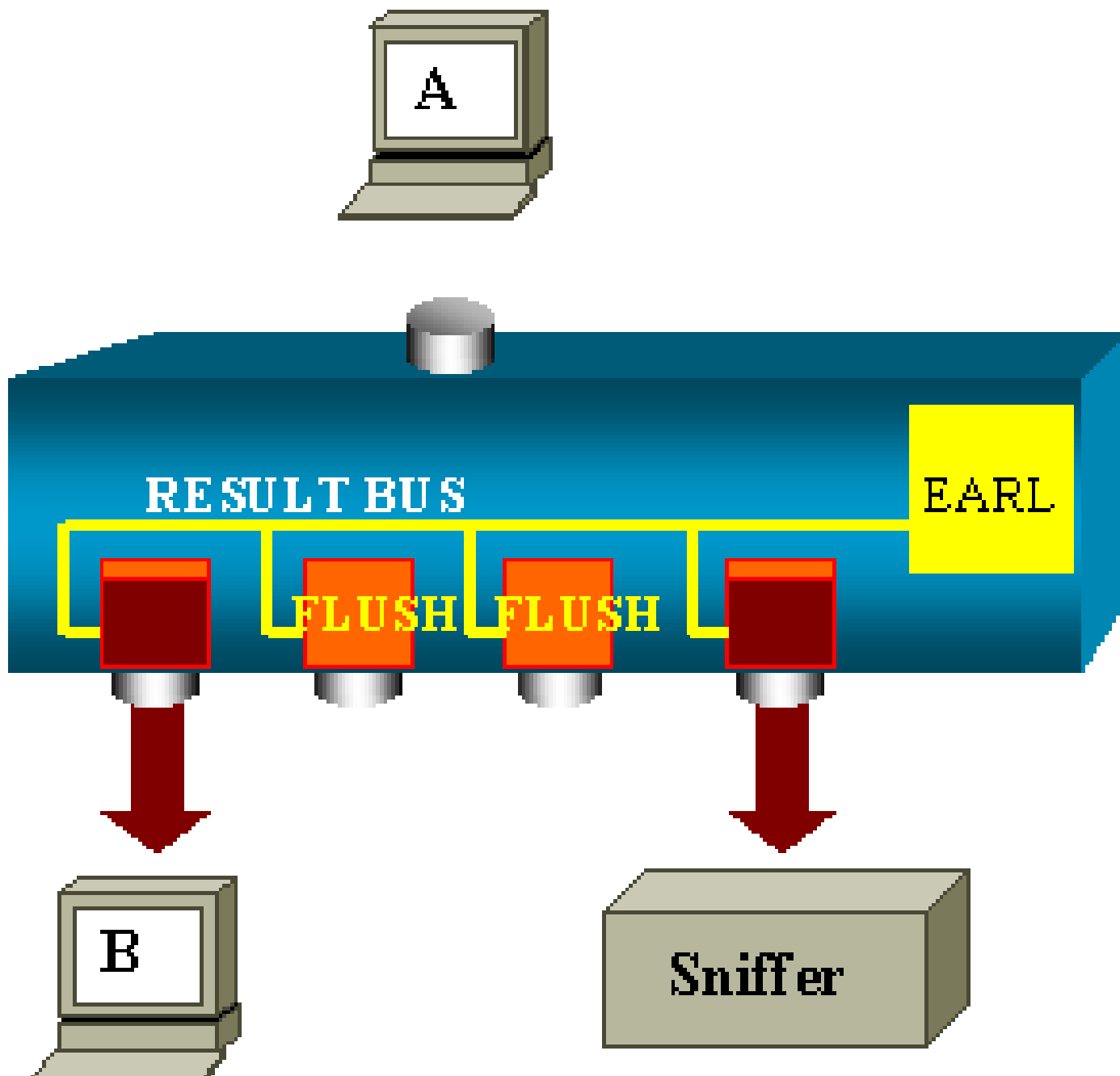
Ogni scheda di linea dello switch inizia a memorizzare questo pacchetto in buffer interni.

Allo stesso tempo, l'EARL (Encoded Address Recognition Logic) riceve l'intestazione del pacchetto e calcola un indice di risultato. L'EARL invia l'indice di risultati a tutte le schede di linea

tramite il bus dei risultati.

La conoscenza di questo indice permette alla scheda di linea di decidere caso per caso se deve eliminare o trasmettere il pacchetto man mano che li riceve nei relativi buffer.





### Conseguenze sulle prestazioni

L'uso di una o più porte per trasmettere i pacchetti non ha alcuna conseguenza sul funzionamento dello switch. Pertanto, in questa architettura, la funzione SPAN non ha alcuna conseguenza sulle prestazioni.

## Domande frequenti e problemi comuni


### Problemi di connettività causati da un'errata configurazione dello SPAN

I problemi di connettività dovuti alla configurazione errata di SPAN si verificano spesso nelle versioni CatOS precedenti alla 5.1. Con queste versioni, è possibile eseguire una sola sessione SPAN.

La sessione rimane nella configurazione, anche quando si disabilita la funzione SPAN. Usando il comando `set span enable`, è possibile riattivare la sessione SPAN memorizzata.

L'azione si verifica spesso a causa di un errore tipografico, ad esempio se l'utente desidera abilitare il protocollo STP. Se la porta di destinazione viene usata per inoltrare il traffico dell'utente, possono verificarsi gravi problemi di connettività.

---

 **Attenzione:** questo problema è ancora in fase di implementazione di CatOS. Prestare molta attenzione alla porta che si sceglie come porta SPAN di destinazione.

---

## Stato attivo/inattivo della porta SPAN di destinazione

Quando le porte sono sottoposte a spanning per il monitoraggio, lo stato della porta viene visualizzato come UP (attivo) o DOWN (inattivo).

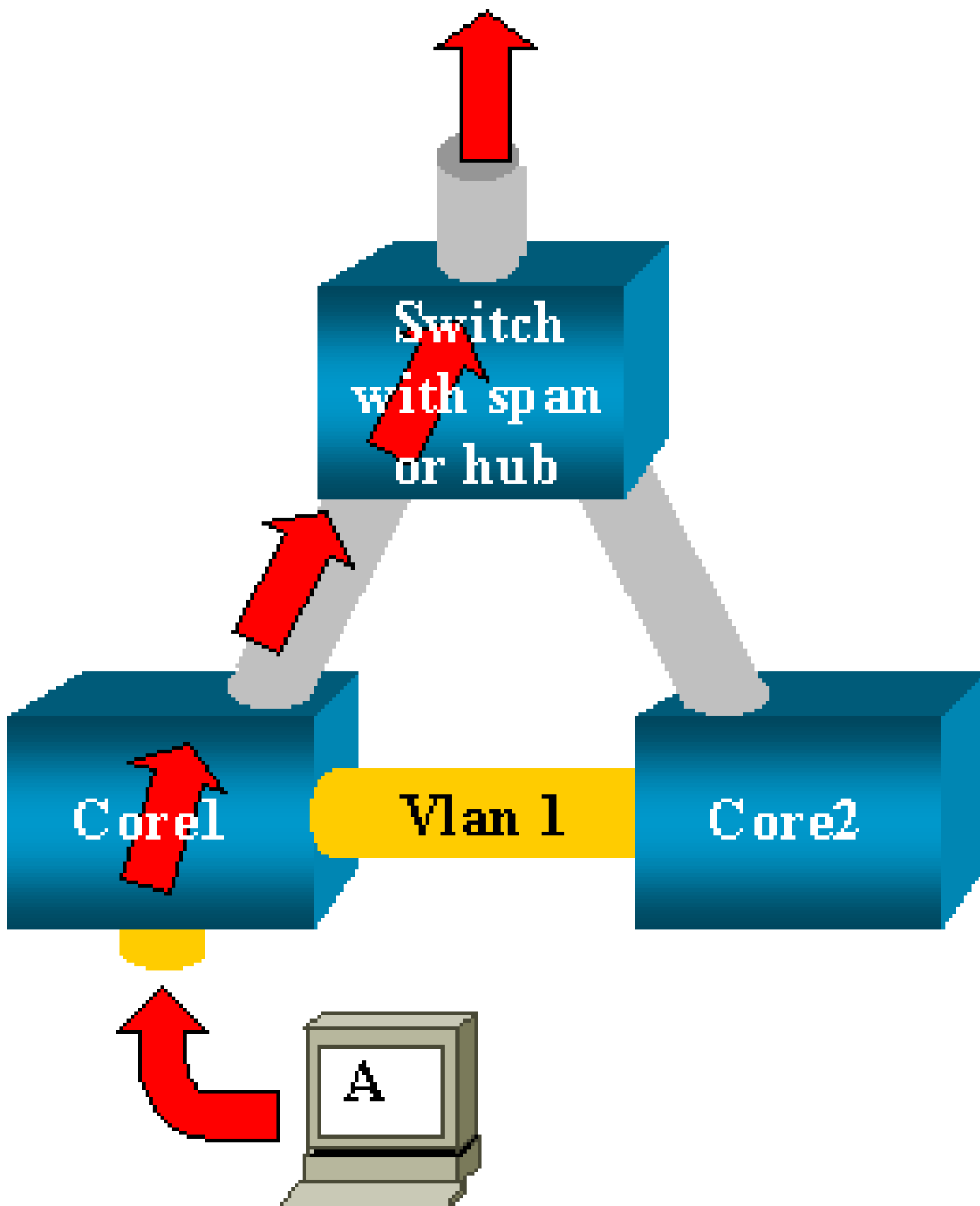
Quando si configura una sessione SPAN per monitorare la porta, per impostazione predefinita l'interfaccia di destinazione mostra lo stato inattivo (monitoraggio).

L'interfaccia mostra lo stato inattivo per evidenziare che al momento la porta non può essere usata come porta di produzione. È normale che la porta di monitoraggio sia attiva o inattiva.

## Perché la sessione SPAN crea un bridging loop?

La creazione di un bridging loop in genere si verifica quando l'amministratore cerca di alterare la funzione RSPAN. Anche un errore di configurazione può causare questo problema.

Ecco uno scenario di esempio:



Due core switch sono collegati da un trunk. In questo caso, ciascuno switch ha diversi server, client o altri bridge connessi.

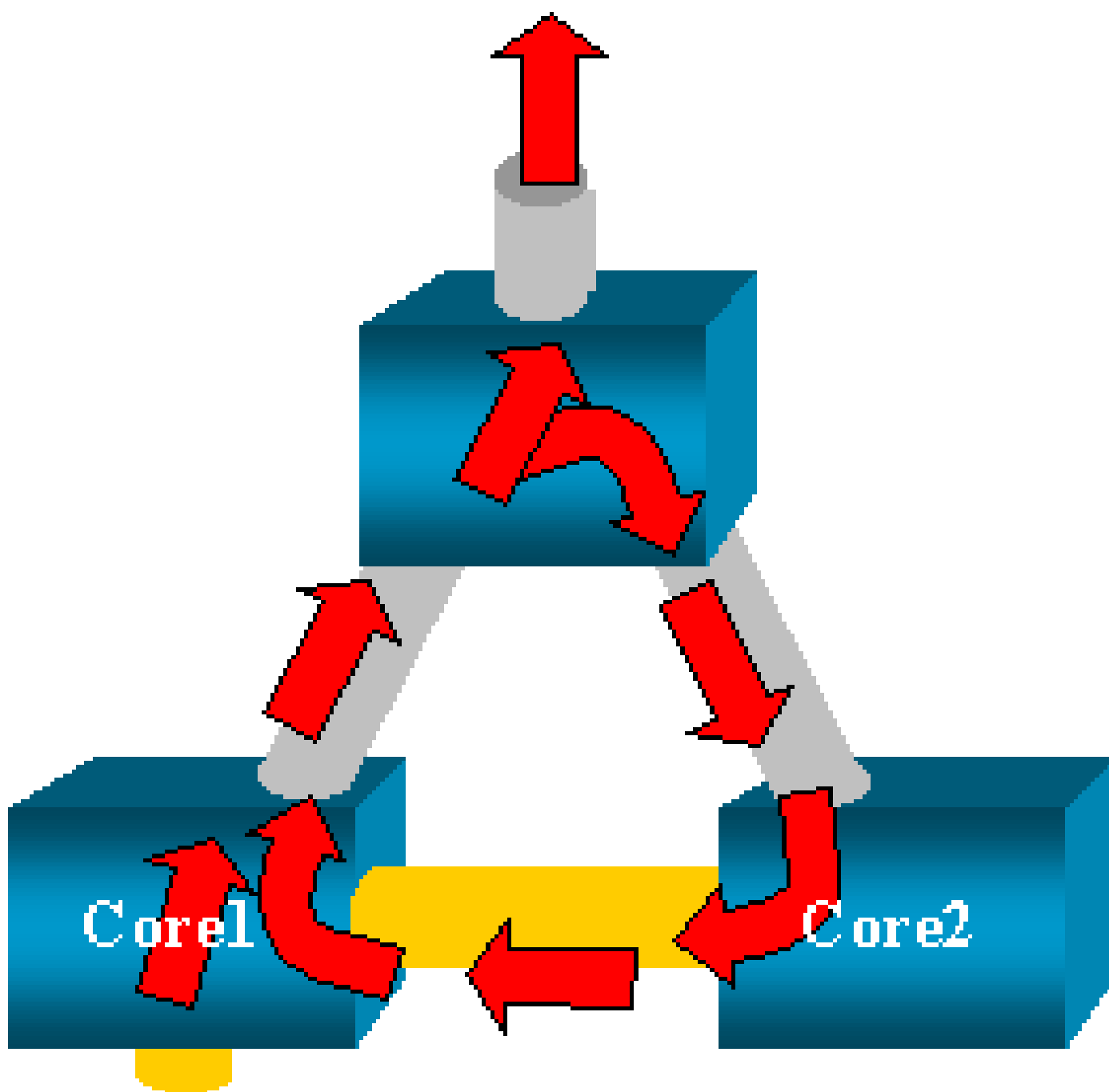
L'amministratore desidera monitorare la VLAN 1, che viene visualizzata su diversi bridge con la funzione SPAN.

L'amministratore crea una sessione SPAN che monitora l'intera VLAN 1 sui singoli core switch e, per unire queste due sessioni, connette la porta di destinazione sullo stesso hub (o sullo stesso switch, con l'uso di un'altra sessione SPAN).


L'obiettivo viene raggiunto. Ciascun singolo pacchetto ricevuto da un core switch sulla VLAN 1 viene copiato sulla porta SPAN e inoltrato a tutte le porte dell'hub. Infine, uno sniffer acquisisce il traffico.

In questo esempio il problema può sorgere dal fatto che il traffico viene nuovamente inoltrato al core 2 tramite la porta SPAN di destinazione.


Il reinserimento del traffico nel core 2 crea un loop di bridging nella VLAN 1. Tenere presente che una porta SPAN di destinazione non esegue STP e non è in grado di evitare un loop di questo tipo.



---

 Nota: a causa dell'introduzione dell'opzione `inpks` (input packets) sul software CatOs, una porta di destinazione SPAN scarta qualsiasi pacchetto in arrivo per impostazione predefinita, impedendo questo scenario di errore. Tuttavia, il problema è ancora potenzialmente presente sui Catalyst serie 2900XL/3500XL Switch.

---

 Nota: anche quando l'opzione `Input penna` impedisce il loop, la configurazione mostrata in questa sezione può causare alcuni problemi nella rete. I problemi di rete possono verificarsi a causa di problemi di acquisizione degli indirizzi MAC associati all'acquisizione abilitata sulla porta di destinazione.

---

## Lo SPAN influisce sulle prestazioni?

Per informazioni sulle conseguenze sulle prestazioni delle piattaforme Catalyst specificate, vedere le sezioni seguenti in questo documento:

- [Catalyst serie 2900XL/3500XL](#)
- [Catalyst serie 4500/4000](#)
- [Catalyst serie 5500/5000 e 6500/6000](#)

## È possibile configurare lo SPAN su una porta EtherChannel?

Se una delle porte del gruppo è una porta SPAN di destinazione, non è possibile formare un EtherChannel. Se si tenta di configurare la funzione SPAN in questa situazione, lo switch visualizza il messaggio:

```
Channel port cannot be a Monitor Destination Port  
Failed to configure span feature
```

È possibile usare una porta di un gruppo EtherChannel come porta SPAN di origine.

## È possibile eseguire più sessioni SPAN allo stesso tempo?

Sui Catalyst serie 2900XL/3500XL Switch, il numero di porte di destinazione disponibili sullo switch è l'unico limite al numero di sessioni SPAN.

Sui Catalyst serie 2950 Switch, è possibile avere una sola porta di monitoraggio assegnata in un dato momento.

Se si seleziona un'altra porta, la porta di monitoraggio precedente viene disabilitata e la porta appena selezionata diventa la nuova porta di monitoraggio.

Sui Catalyst serie 4500/4000, 5500/5000 e 6500/6000 Switch con CatOS 5.1 e versioni



successive, è possibile avere più sessioni SPAN simultanee.

Vedere le sezioni [Creazione di più sessioni simultanee](#) e [Riepilogo delle funzioni e limitazioni](#) in questo documento.

## Errore limite delle sessioni locali superato

Il messaggio di errore "% Local Session Limit Has Been Exceeded" (Il limite delle sessioni locali % è stato superato) viene visualizzato quando la sessione SPAN consentita supera il limite definito di Supervisor Engine:

```
% Local Session limit has been exceeded
```

I Supervisor Engine possono gestire un numero limitato di sessioni SPAN. Per ulteriori informazioni, fare riferimento alla sezione [Limitazioni delle sessioni SPAN, RSPAN ed ERSPAN locali in Configurazione di SPAN, RSPAN ed ERSPAN locale](#).

## Impossibile eliminare una sessione SPAN sul modulo di servizio VPN perché in uso

Il messaggio di errore "% Session [Session No:] Used by Service Module" (% sessione [N. sessione]: utilizzato dal modulo di servizio) viene visualizzato quando il modulo VPN (Virtual Private Network) è inserito nello chassis, dove è già presente un modulo switch fabric.

Il software Cisco IOS crea automaticamente una sessione SPAN per il modulo di servizio VPN per gestire il traffico multicast.

Usare questo comando per eliminare la sessione SPAN creata dal software per il modulo di servizio VPN:

```
<#root>
```

```
Switch(config)#
```

```
no monitor session session_number service-module
```



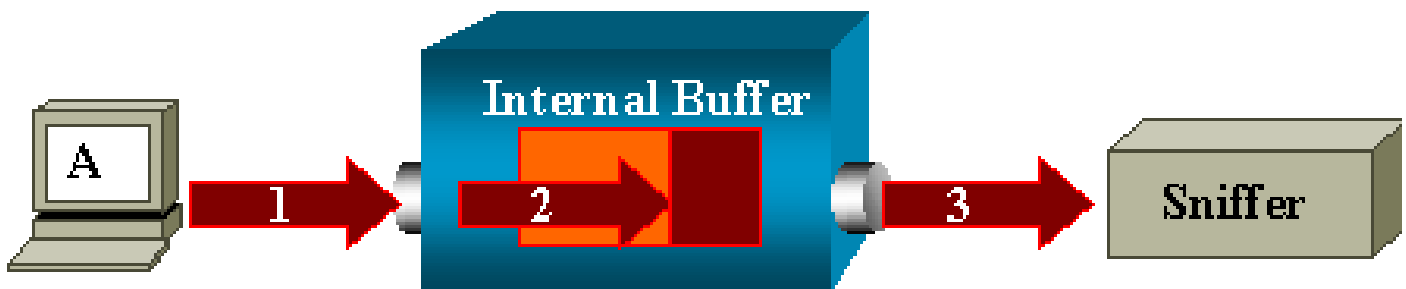
Nota: se si elimina la sessione, il modulo del servizio VPN scarta il traffico multicast.

---

## Perché non è possibile acquisire pacchetti danneggiati con lo SPAN?

Non è possibile acquisire pacchetti danneggiati con la funzione SPAN a causa della logica generale con cui funzionano gli switch. Quando un pacchetto attraversa uno switch, si verificano questi eventi:

1. Il pacchetto raggiunge la porta di ingresso.
2. Il pacchetto viene memorizzato in almeno un buffer.
3. Infine, il pacchetto viene nuovamente trasmesso sulla porta di uscita.



Se lo switch riceve un pacchetto danneggiato, la porta di ingresso in genere lo elimina. Pertanto, il pacchetto non arriva alla porta di uscita.

L'acquisizione del traffico in uno switch non è completamente trasparente.

Analogamente, se nello scenario descritto in questa sezione si rileva un pacchetto danneggiato sullo sniffer, se ne può dedurre che l'errore è stato generato nel passaggio 3, sul segmento di uscita.

Se si sospetta che un dispositivo invii pacchetti danneggiati, è possibile scegliere di mettere l'host di invio e lo sniffer su un hub. L'hub non esegue controlli sugli errori.

Pertanto, a differenza dello switch, l'hub non elimina i pacchetti. In questo modo, è possibile vedere tutti i pacchetti.

## Errore: % sessione 2 utilizzata dal modulo del servizio

Il messaggio di errore "% Session 2 used by service module" (% sessione 2 utilizzata dal modulo di servizio) viene visualizzato nel seguente scenario: quando viene installato un modulo FWSM (Firewall Service Module), o installato e successivamente rimosso, sui Catalyst 6500 viene abilitata automaticamente la funzione SPAN Reflector.

La funzione SPAN Reflector usa una sessione SPAN dello switch.

Per disattivare questa funzione, usare il comando `no monitor session service module` in modalità di configurazione sui Catalyst 6500 e immettere subito dopo la configurazione SPAN desiderata.

## Eliminazione dei pacchetti sulla porta reflector

Alla porta reflector viene inoltrata una copia del traffico inviato e ricevuto su tutte le porte di origine monitorate. Se una porta reflector viene usata oltre la sua capacità, può crearsi una congestione.

Ciò potrebbe influire sull'inoltro del traffico su una o più porte di origine.

Se la larghezza di banda della porta reflector non è adeguata al volume di traffico delle porte di

origine corrispondenti, i pacchetti in eccesso vengono eliminati.

La velocità di una porta 10/100 è 100 Mbps. La velocità di una porta Gigabit è 1 Gbps.

Sui Catalyst 6500 la sessione SPAN viene usata sempre con un modulo FWSM

Quando si usa Supervisor Engine 720 con un FWSM nello chassis e Cisco Native IOS, viene usata per impostazione predefinita una sessione SPAN. Se si usa il comando show monitor per verificare le sessioni, il comando restituisce la sessione 1 come sessione usata:

```
<#root>
```

```
Cat6K#
```

```
show monitor
```

```
Session 1
```

```
-----
```

```
Type : Service Module Session
```

Quando lo chassis Catalyst 6500 contiene un blade firewall, questa sessione viene installata automaticamente per copiare il traffico multicast del dispositivo, in quanto il modulo FWSM non supporta questa funzionalità.

Se i flussi multicast provenienti dal modulo FWSM devono essere copiati su più schede di linea sul layer 3, la sessione copia in automatico il traffico diretto al supervisor tramite un canale del fabric.

Se il traffico multicast è generato a monte del modulo FWSM, è necessario usare il reflector SPAN.

Se si posiziona l'origine del traffico multicast sulla VLAN esterna, il reflector SPAN non è necessario. Il reflector SPAN non è compatibile con le BPDU di bridging che attraversano il modulo FWSM.

Per disabilitare il reflector SPAN, usare il comando no monitor session service module.

È possibile usare lo stesso ID per una sessione SPAN e una sessione RSPAN nello stesso switch?

No, non è possibile utilizzare lo stesso ID per una normale sessione SPAN e una sessione RSPAN di destinazione. Ciascuna sessione SPAN o RSPAN deve avere un ID univoco.

È possibile eseguire una sessione RSPAN su domini VTP diversi?

Sì. Una sessione RSPAN può includere domini VTP diversi. Tuttavia, verificare che la RSPAN VLAN sia presente nei database di questi domini VTP.

Inoltre, accertarsi che ciascun dispositivo di layer 3 sia presente nel percorso tra la sessione di origine e la sessione di destinazione.

È possibile eseguire una sessione RSPAN su WAN o reti diverse?

No. La sessione RSPAN non può essere eseguita su nessun dispositivo di layer 3 in quanto è una funzione progettata per la rete LAN e quindi per il layer 2.

Per monitorare il traffico su una WAN o su reti diverse, occorre usare la funzione Encapsulate Remote SwitchPort Analyzer (ERSPAN).

La funzione ERSPAN consente di avere porte di origine, VLAN di origine e porte di destinazione posizionate su switch diversi e quindi di monitorare da remoto più switch appartenenti alla rete.

La funzione ERSPAN è composta da una sessione ERSPAN di origine, dal traffico ERSPAN indirizzabile con incapsulamento GRE e da una sessione ERSPAN di destinazione.

È possibile configurare separatamente le sessioni ERSPAN di origine e di destinazione su switch diversi.

Attualmente, la funzione ERSPAN è supportata in:

- Supervisor 720 con PFC3B o PFC3BXL con Cisco IOS Software Release 12.2(18)SXE o versioni successive
- Supervisor 720 con PFC3A con versione hardware 3.2 o successive e con Cisco IOS Software Release 12.2(18)SXE o versioni successive.

Per ulteriori informazioni sulla funzione ERSPAN, fare riferimento a [Configurazione di SPAN, Remote SPAN \(RSPAN\) e Encapsulated RSPAN locale - Guida alla configurazione dei Catalyst 6500 con Cisco IOS Software 12.2SX](#).

È possibile avere contemporaneamente una sessione RSPAN di origine e di destinazione sullo stesso Catalyst Switch?

No. Se la sessione RSPAN di origine e la sessione RSPAN di destinazione si trovano sullo stesso switch, RSPAN non può funzionare.

Se si configura una sessione RSPAN di origine con una specifica RSPAN VLAN e la sessione RSPAN di destinazione di tale VLAN è configurata sullo stesso switch, la porta di destinazione della sessione RSPAN di destinazione non trasmetterà i pacchetti acquisiti dalla sessione RSPAN di origine, a causa delle limitazioni dell'hardware. Questo scenario non è supportato sugli switch serie 4500 e serie 3750.

Il problema è documentato dall'ID bug Cisco [CSCeg08870](#) (solo utenti registrati).

Ecco un esempio:

```
monitor session 1 source interface Gi6/44
monitor session 1 destination remote vlan 666
monitor session 2 destination interface Gi6/2
monitor session 2 source remote vlan 666
```

Per risolvere il problema, usare la funzione SPAN normale.

## Impossibile raggiungere l'analizzatore di rete o il dispositivo di sicurezza connesso alla porta SPAN di destinazione

Come da progetto, una porta SPAN di destinazione trasmette esclusivamente il traffico richiesto per la sessione SPAN.

In caso sia necessario raggiungere l'analizzatore di rete o il dispositivo di sicurezza, ossia ottenere l'IP, tramite la porta SPAN di destinazione, è necessario abilitare l'inoltro del traffico in ingresso.

Quando il traffico in ingresso è abilitato, la porta SPAN di destinazione accetta i pacchetti in arrivo, che potrebbero essere contrassegnati con tag a seconda della modalità di incapsulamento usata, e li commuta normalmente.

Quando si configura una porta SPAN di destinazione, è possibile specificare se abilitare o meno l'inoltro del traffico in ingresso e quale VLAN usare per commutare i pacchetti in arrivo senza tag.

Se si usa l'incapsulamento ISL, non è necessario specificare una VLAN di ingresso; tutti i pacchetti incapsulati ISL hanno infatti tag VLAN.

Anche se la porta prevede un inoltro STP, il protocollo STP non viene usato; adottare quindi le opportune cautele quando si configura questa funzione per non introdurre un loop spanning-tree nella rete.

Quando su una porta SPAN di destinazione sono specificati sia un incapsulamento in ingresso che un incapsulamento trunk, la porta inoltra i pacchetti a tutte le VLAN attive.

Non è consentito configurare come VLAN di ingresso una VLAN che non è stata ancora creata.

```
monitor session session_number destination interface interface [encapsulation {isl | dot1q}] in
entrata [vlan vlan_IDs]
```

L'esempio mostra come configurare una porta di destinazione con pacchetti di ingresso e di incapsulamento 802.1q che usano la VLAN 7 nativa.

<#root>

```
Switch(config)#
```

```
monitor session 1 destination interface fastethernet 5/48
encapsulation dot1q ingress vlan 7
```

In questa configurazione, il traffico proveniente dalle porte SPAN di origine associate alla sessione 1 viene copiato dall'interfaccia Fast Ethernet 5/48, con incapsulamento 802.1q.

Il traffico in arrivo è accettato e commutato, i pacchetti senza tag sono classificati nella VLAN 7.

## Informazioni correlate

- [Come configurare le funzioni SPAN e RSPAN sui Cisco Catalyst 4500 Switch con software Cisco IOS](#)
- [Una porta SPAN di destinazione viene visualizzata come "non connessa" e non comunica con il resto della rete](#)
- [Switch - Supporto dei prodotti](#)
- [Supporto della tecnologia di switching LAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## 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).