

# Esempio di configurazione degli switch Catalyst Express serie 500

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione iniziale dello switch](#)

[SmartPort](#)

[Ruoli Smartport](#)

[Applicazione dei ruoli Smartport alle porte](#)

[Restrizioni](#)

[Applicazione di un ruolo Smartports a una porta singola](#)

[Applicazione di un ruolo Smartports a tutte le porte](#)

[Creazione/eliminazione di VLAN](#)

[Tipi di VLAN](#)

[Modifica dell'appartenenza della VLAN](#)

[Configura EtherChannel](#)

[Configurazione del routing tra VLAN con un router Cisco](#)

[Configurazione di SPAN \(Switched Port Analyzer\)](#)

[Ripristino delle impostazioni predefinite dello switch Catalyst Express 500](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene descritto come configurare gli switch Cisco Catalyst Express serie 500 per i ruoli Smartport, le VLAN, EtherChannel, Switch Port Analyzer (SPAN) e come effettuare il routing tra VLAN con gli switch Cisco Catalyst Express serie 500.

## [Prerequisiti](#)

### [Requisiti](#)

Cisco raccomanda la conoscenza dei seguenti argomenti:

- EtherChannel

- Routing interVLAN
- SPAN

Configurare lo switch Cisco Catalyst serie 5500 con le impostazioni di rete iniziali come indicato nella sezione [Configurazione iniziale dello switch](#) in questo documento.

Per informazioni sui diversi modelli e sulle funzionalità supportate negli switch Cisco Catalyst serie 5500, consultare il foglio dati [sugli switch Cisco Catalyst serie 500](#).

## [Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst Express 500G-12TC con software Cisco IOS® versione 12.2(25)FY
- Cisco 2800 Router che supporta IEEE 802.1Q Trunk Encapsulation.
- Switch Cisco Catalyst 3750 che supportano l'incapsulamento trunk 802.1Q.

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

## [Convenzioni](#)

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## [Configurazione iniziale dello switch](#)

Per eseguire la configurazione iniziale dello switch, attenersi alla seguente procedura. Per ulteriori informazioni sulla procedura di configurazione, consultare la [Guida introduttiva agli switch Catalyst Express 500](#).

1. Accertarsi che lo switch non sia collegato ad alcun elemento.
2. Accendere lo switch.
3. Attendere che il LED SETUP lampeggi in verde.
4. Fare clic su **Imposta**. Il LED della porta dello switch inizia a lampeggiare in verde.
5. Quando il LED della porta dello switch lampeggia in verde, collegare il PC a tale porta. La scheda LAN del PC deve essere configurata per ottenere l'indirizzo IP tramite DHCP. I LED sul PC e sulla porta dello switch lampeggiano in verde mentre lo switch configura la connessione (l'operazione richiede circa un minuto).
6. Aprire un browser Web. Se il browser non attiva automaticamente la GUI, completare la procedura seguente: Usare il comando **ipconfig** per visualizzare l'allocazione dinamica degli indirizzi.

```
C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

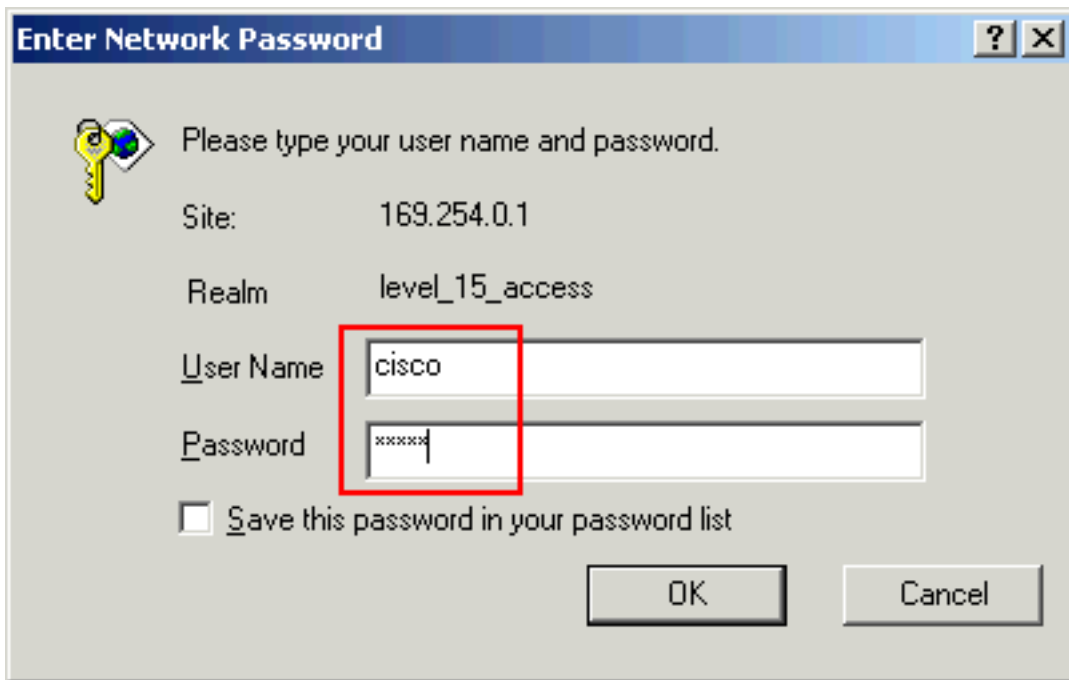
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : apac.cisco.com
    IP Address. . . . . : 169.254.0.2
    Subnet Mask . . . . . : 255.255.255.248
    Default Gateway . . . . . : 169.254.0.1
```

Lo switch configura il proprio indirizzo di gestione come gateway predefinito per la scheda di rete LAN del PC. **Nota:** per il software Cisco IOS serie **FY**, l'indirizzo IP di gestione è 10.0.0.1. Per il software Cisco IOS serie **SEG**, l'indirizzo IP è 169.254.0.1. Dal browser, passare all'indirizzo IP indicato. Ad esempio, <http://169.254.0.1>.

- 7. Immettere le impostazioni di rete e le impostazioni facoltative (se necessario). Fare clic su **Submit** (Invia) per salvare le modifiche e completare la configurazione di base.

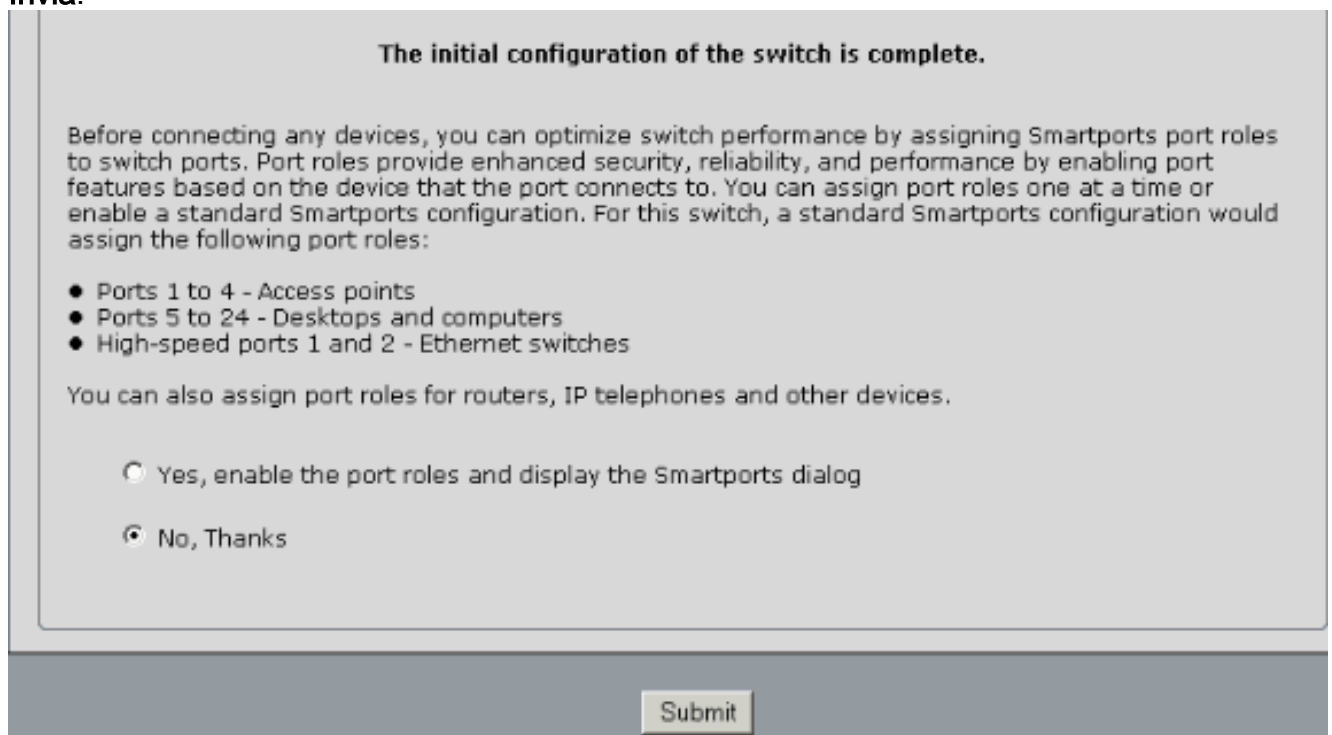
- 8. Immettere il nome utente e la password configurati per continuare la configurazione dello



The image shows a Windows-style dialog box titled "Enter Network Password". It contains a key icon and the text "Please type your user name and password." Below this, there are fields for "Site" (169.254.0.1) and "Realm" (level\_15\_access). The "User Name" field contains "cisco" and the "Password" field contains "xxxxxx". A red rectangle highlights the "User Name" and "Password" fields. At the bottom, there is a checkbox labeled "Save this password in your password list" which is unchecked, and two buttons: "OK" and "Cancel".

switch.

9. Per la finestra di dialogo Smartports: Per accettare i ruoli porta predefiniti, fare clic su **Sì** e su **Sottometti**. Viene visualizzata la finestra Smartports. In questa finestra è possibile modificare i ruoli predefiniti o applicare nuovi ruoli porta. Per applicare manualmente i ruoli Smartports, fare clic su **No** e su **Invia**.



The image shows a dialog box titled "The initial configuration of the switch is complete." It contains the following text: "Before connecting any devices, you can optimize switch performance by assigning Smartports port roles to switch ports. Port roles provide enhanced security, reliability, and performance by enabling port features based on the device that the port connects to. You can assign port roles one at a time or enable a standard Smartports configuration. For this switch, a standard Smartports configuration would assign the following port roles:"

- Ports 1 to 4 - Access points
- Ports 5 to 24 - Desktops and computers
- High-speed ports 1 and 2 - Ethernet switches

You can also assign port roles for routers, IP telephones and other devices.

Yes, enable the port roles and display the Smartports dialog

No, Thanks

Submit

10. Riavviare lo switch senza spegnere l'apparecchio.

Restart / Reset

Restart the switch with its current settings.

Reset the switch to factory defaults, and then restart the switch.

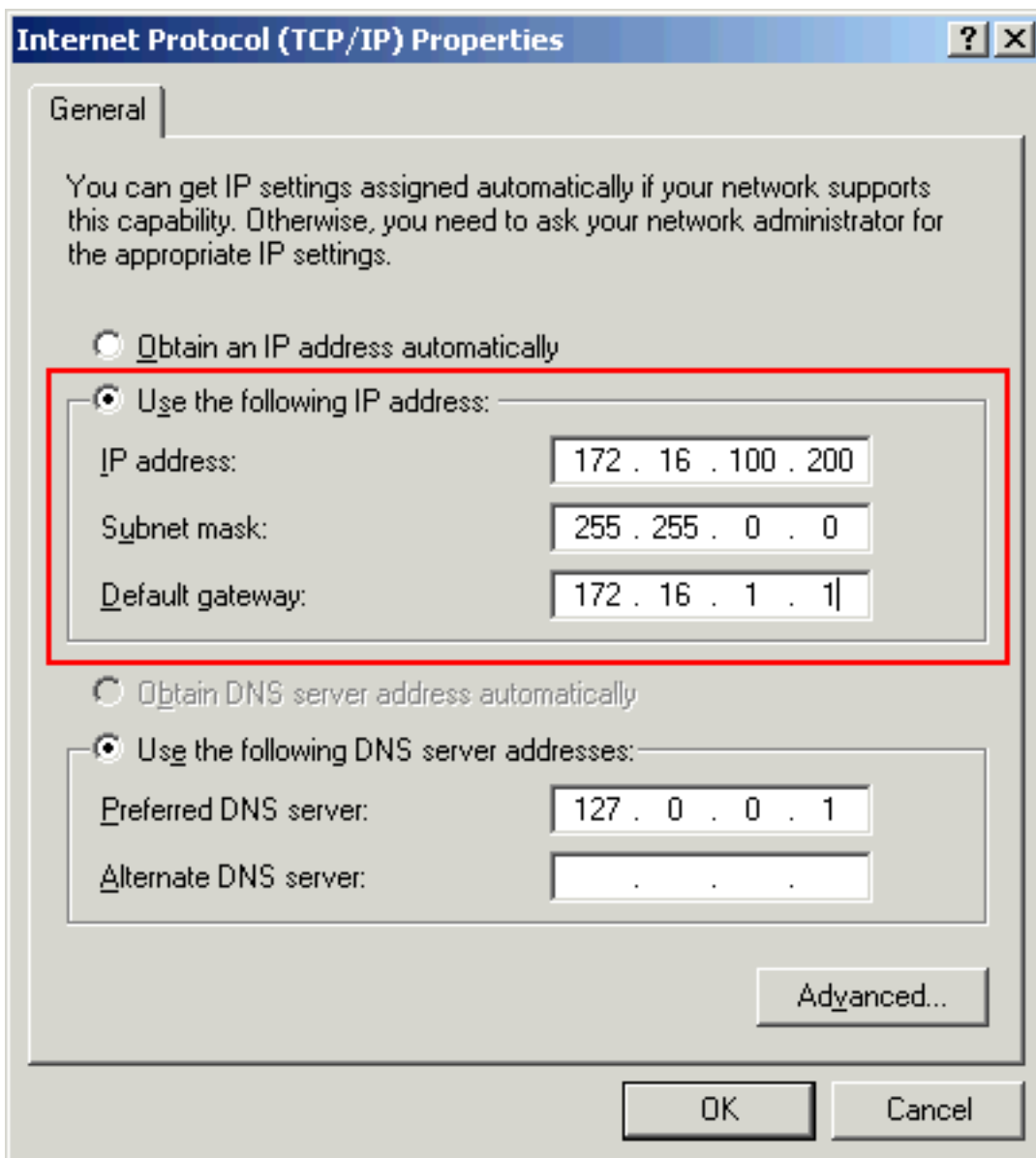
Submit Cancel

Lo switch viene ricaricato automaticamente tra 60 secondi. Un contatore indica il tempo rimanente per il ricaricamento.

Restart / Reset

Device will be reloaded in 59 second(s).

11. Chiudere il browser Web e riconfigurare la scheda LAN con un indirizzo IP nella stessa subnet del nuovo indirizzo di gestione dello



switch.

12. Dopo l'accensione dello switch, aprire un browser Web e visitare il sito [http://<CE500\\_Management\\_IP\\_Address>](http://<CE500_Management_IP_Address>). Ad esempio, <http://172.16.100.100>. **Nota:** al termine della configurazione iniziale, lo switch può essere gestito tramite qualsiasi porta configurata per la stessa VLAN di quella dell'indirizzo IP di gestione.

## SmartPort

### Ruoli Smartport

Le porte Smartport sono porte switch preconfigurate che offrono miglioramenti di rete, QoS (Quality of Service) e sicurezza consigliati da Cisco. Gli switch Catalyst Express serie 500 hanno diversi ruoli Smartport. Ogni ruolo porta è solo un modello di configurazione. Grazie a questi modelli, gli utenti possono configurare in modo coerente e affidabile funzioni essenziali di sicurezza, disponibilità e QoS con il minimo sforzo ed esperienza. I ruoli Smartport semplificano la configurazione delle funzionalità critiche.

I ruoli delle porte si basano sul tipo di dispositivi da connettere alle porte dello switch. Ad esempio, il ruolo Porta desktop è specifico per le porte degli switch connesse a PC desktop o portatili.

Ruol	Descrizione
------	-------------

o Smartport	
Desktop	<p>Applica questo ruolo alle porte connesse a dispositivi desktop, ad esempio PC desktop, workstation, notebook e altri host basati su client.</p> <ul style="list-style-type: none"> <li>• Ottimizzato per la connettività desktop</li> <li>• Impostazione VLAN configurabile</li> <li>• Sicurezza porta abilitata per limitare l'accesso non autorizzato alla rete</li> </ul>
Switch	<p>Applica questo ruolo alle porte connesse ad altri switch.</p> <ul style="list-style-type: none"> <li>• Configurata come porta uplink su uno switch backbone per una convergenza rapida</li> <li>• Consente il trunking 802.1Q</li> <li>• VLAN nativa configurabile</li> </ul>
Router	<p>Applicare questo ruolo alle porte connesse ai dispositivi WAN connessi a Internet, ad esempio router e switch di layer 3 con funzionalità del servizio di routing, firewall o concentratori VPN.</p> <ul style="list-style-type: none"> <li>• Configurato per una connessione ottimale a un router o a un firewall per la connettività WAN</li> <li>• Consente il trunking 802.1Q</li> <li>• VLAN nativa configurabile</li> </ul>
IP Phone e desktop	<p>Applica questo ruolo alle porte connesse ai telefoni IP. È possibile collegare un dispositivo desktop, ad esempio un PC, al telefono IP. Sia il telefono IP che il PC connesso hanno accesso alla rete e a Internet tramite la porta dello switch. Questo ruolo assegna la priorità al traffico vocale rispetto al traffico dati per garantire una ricezione chiara della voce sui telefoni IP.</p> <ul style="list-style-type: none"> <li>• QoS ottimizzato per configurazioni IP Phone + desktop</li> <li>• Il traffico vocale viene indirizzato sulla VLAN Cisco-Voice</li> <li>• VLAN dati configurabile</li> <li>• Il livello QoS garantisce la precedenza del traffico VoIP (Voice over IP)</li> <li>• Sicurezza porta abilitata per limitare l'accesso non autorizzato alla rete</li> </ul>
Access Point	<p>Applica questo ruolo alle porte dello switch che si connettono a punti di accesso wireless (AP) e PoE non compatibili con Power over Ethernet (PoE). Al punto di accesso sono collegati dispositivi mobili, ad esempio laptop wireless.</p> <ul style="list-style-type: none"> <li>• Configurato per la connessione ottimale a un punto di accesso wireless</li> </ul>

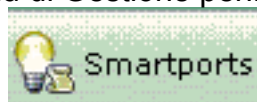
	<ul style="list-style-type: none"> <li>• Consente il trunking 802.1Q</li> <li>• VLAN nativa configurabile</li> </ul> <p><b>Nota:</b> le funzionalità dei Cisco Wireless Bridge sono più simili a quelle di uno switch. Cisco consiglia di assegnare allo <b>switch</b> il ruolo di SmartPort per i bridge wireless.</p>
Server	<p>Applicare questo ruolo alle porte connesse ai server che forniscono servizi di rete, ad esempio server Exchange, server di collaborazione, server terminal, file server, server DHCP (Dynamic Host Configuration Protocol), server PBX (IP Private Branch Exchange) e così via. Questo ruolo è riservato alle porte Gigabit o non Gigabit, in base al tipo di server da connettere.</p> <ul style="list-style-type: none"> <li>• VLAN configurabile</li> <li>• Sicurezza porta abilitata per limitare l'accesso non autorizzato alla rete</li> </ul> <p>Questo ruolo assegna la priorità al traffico del server come trusted, critical, business o standard, in base alla funzione del server.</p> <ul style="list-style-type: none"> <li>• <b>Trusted:</b> per l'uso con Cisco CallManager Express. La stessa impostazione QoS di Voice (traffico VoIP con priorità).</li> <li>• <b>Critical:</b> per i server critici con QoS impostato su un valore superiore a quello predefinito.</li> <li>• <b>Business</b> - Impostazione di default. QoS è superiore al traffico Internet del desktop.</li> <li>• <b>Standard:</b> per server impostati allo stesso livello del normale traffico Internet desktop.</li> </ul>
Stampante	<p>Applica questo ruolo alle porte switch che si connettono a una stampante, ad esempio una stampante di rete o un server di stampa esterno. Questo ruolo impedisce al traffico della stampante di influire sul traffico di dati vocali e critici.</p> <ul style="list-style-type: none"> <li>• Le impostazioni QoS per la stampante sono le stesse di Desktop, Access Point e Standard Server</li> <li>• VLAN configurabile</li> <li>• Sicurezza porta abilitata per limitare l'accesso non autorizzato alla rete</li> </ul>
Guest	<p>Applica questo ruolo alle porte connesse ai dispositivi desktop e agli access point per fornire l'accesso wireless guest.</p> <ul style="list-style-type: none"> <li>• Gli ospiti possono accedere a Internet, ma non alla rete aziendale.</li> <li>• Tutte le porte guest vengono posizionate sulla VLAN Cisco-Guest.</li> <li>• Sicurezza porta abilitata per limitare l'accesso non autorizzato alla rete.</li> </ul>



Other (Altro)	<p>Applicare questo ruolo alle porte dello switch se non si desidera assegnare un ruolo specializzato sulla porta. Questo ruolo può essere utilizzato nelle connessioni a dispositivi guest o visitatori, stampanti, desktop, server e telefoni IP. Consente una connettività flessibile di dispositivi non specificati.</p> <ul style="list-style-type: none"> <li>• VLAN configurabile</li> <li>• Nessun criterio di protezione</li> <li>• Nessun criterio QoS</li> </ul>
Diagnostica	I clienti possono connettere dispositivi di diagnostica per monitorare il traffico su altri switch (configurabili solo con Cisco Network Assistant).

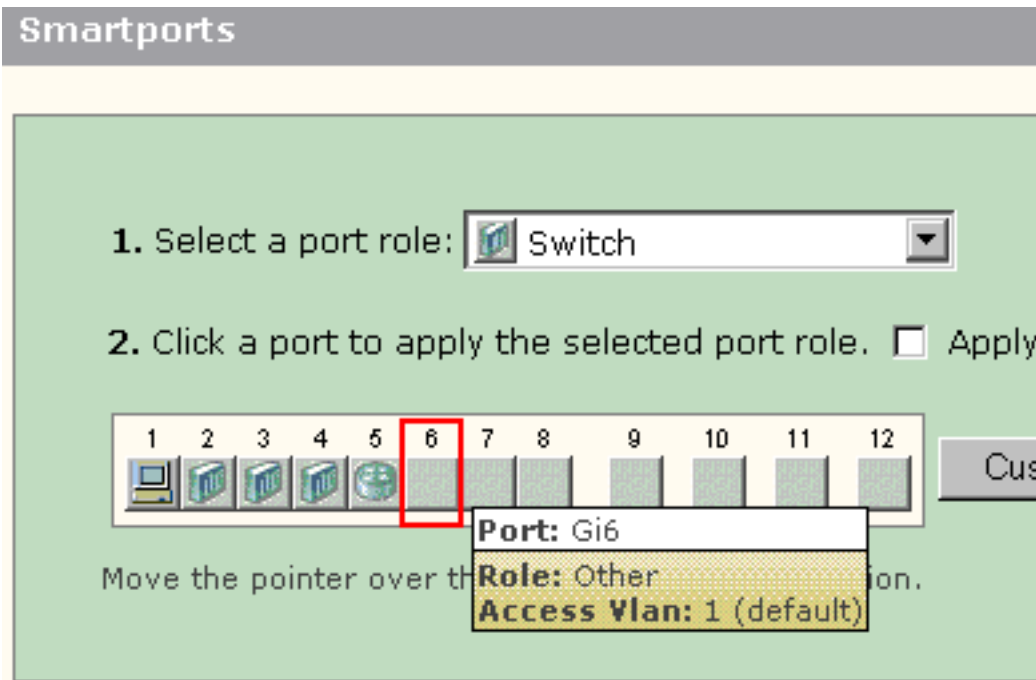
## Applicazione dei ruoli Smartport alle porte

Utilizzare la finestra Smartports per applicare i ruoli delle porte alle porte dello switch. Selezionare **Configura > Smartports** dal menu di Gestione periferiche per visualizzare questa finestra. È inoltre



possibile fare clic su **Smartports** dalla barra degli strumenti di Gestione dispositivi.

Nella finestra Smartports è possibile visualizzare il ruolo Smartports applicato a ogni porta. Spostare il puntatore su una porta per visualizzarne il numero, il ruolo Smartports e l'ID VLAN (appartenenza alla VLAN).



Prima di utilizzare le porte Smartport, stabilire a quale porta dello switch si desidera connettersi e a quale tipo di dispositivo. È possibile applicare un ruolo Smartports a una [porta specifica](#) o a [tutte le porte](#) dello switch.

## Restrizioni

- È consigliabile non modificare impostazioni di porta specifiche dopo aver abilitato un ruolo Smartports in una porta. Qualsiasi modifica apportata alle impostazioni della porta può alterare l'efficacia del ruolo Smartports.
- Non applicare il ruolo Desktop alle porte connesse a switch, router o punti di accesso.
- Lo **switch di ruolo Smartport** abilita automaticamente il trunking 802.1Q sulla porta. Se uno switch remoto non supporta il trunking 802.1Q o il trunking è disattivato manualmente, lo stato dello spanning tree della porta sullo switch remoto passa al blocco per incoerenza del tipo. Se lo switch remoto è il bridge radice, la porta dello switch non passa alla modalità di blocco. In questo caso, lo stato del trunk della porta dello switch è ON su entrambe le estremità degli switch, ma non vi è alcuna comunicazione tra gli switch tramite queste porte. Nessun messaggio diagnostico visualizzato sul dispositivo Catalyst Express 500. **Uscita da switch remoto**

```
%SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet2/0/1 VLAN2.
%SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet2/0/1 on VLAN0002. Inconsistent port
type.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
```

```
Switch2#show spanning-tree vlan 2
```

```
VLAN0002
```

```
Spanning tree enabled protocol ieee
Root ID    Priority    32770
Address    0012.01c7.7c80
This bridge is the root
Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

Bridge ID  Priority    32770 (priority 32768 sys-id-ext 2)
Address    0012.01c7.7c80
```

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300

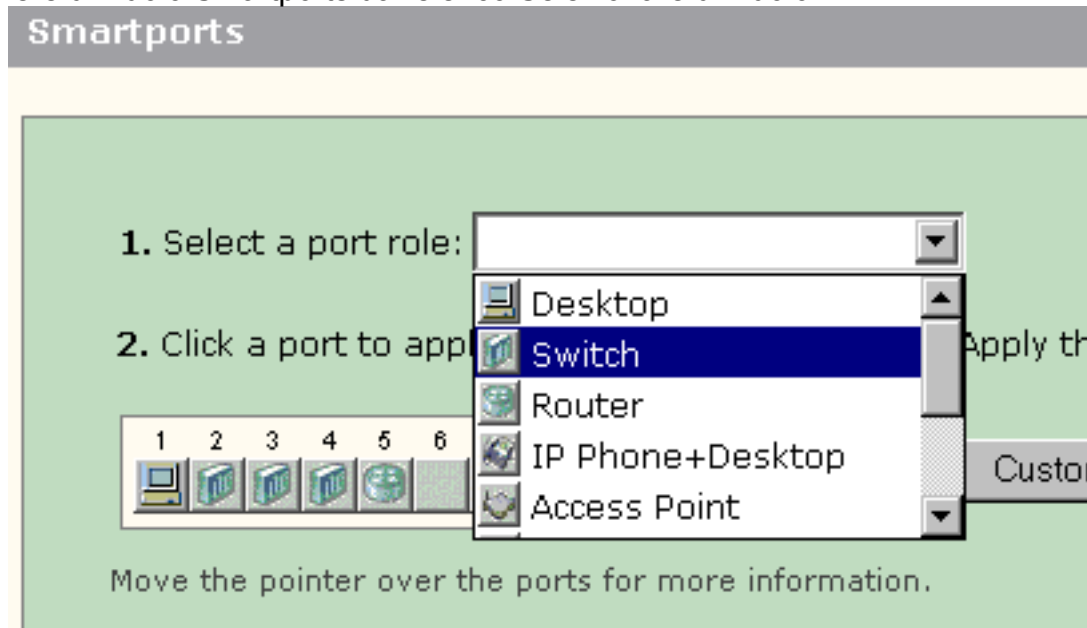
Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----	-----	-----	-----	-----	-----	-----
Gi2/0/1	Desg	BKN*4		128.53		P2p *TYPE_Inc

- Il **router di ruolo Smartport** abilita automaticamente il trunking 802.1Q sulla porta. Se si usa l'interfaccia principale del router remoto, verificare che l'interfaccia del router sia parte della VLAN nativa della porta dello switch. L'interfaccia del router può essere sottointerfacciata per fornire il routing tra VLAN per lo switch Cisco Catalyst Express 500. Per i dettagli della configurazione, vedere la sezione [Configurazione del routing tra VLAN con un router Cisco](#) di questo documento.
- Per applicare il ruolo **IP Phone+Desktop** Smartport alle porte, è necessario disporre di una VLAN aggiuntiva chiamata **Cisco-Voice** (con distinzione tra maiuscole e minuscole).
- Per applicare il ruolo **Guest** Smartport alle porte, è necessario disporre di una VLAN aggiuntiva denominata **Cisco-Guest** (con distinzione tra maiuscole e minuscole).
- Non applicare il ruolo Altro alle porte connesse a dispositivi di rilevamento sniffer o intrusioni.

## [Applicazione di un ruolo Smartports a una porta singola](#)

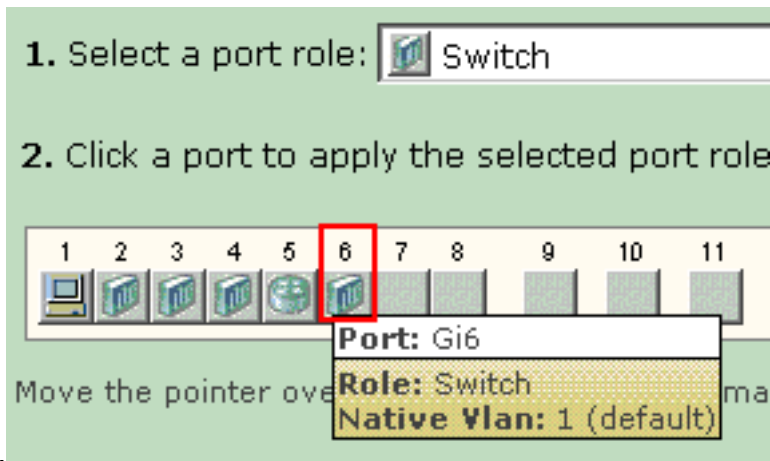
Per applicare un ruolo Smartports a una porta specifica, completare la procedura seguente:

1. Scegliere un ruolo Smartports dall'elenco Selezionare un ruolo



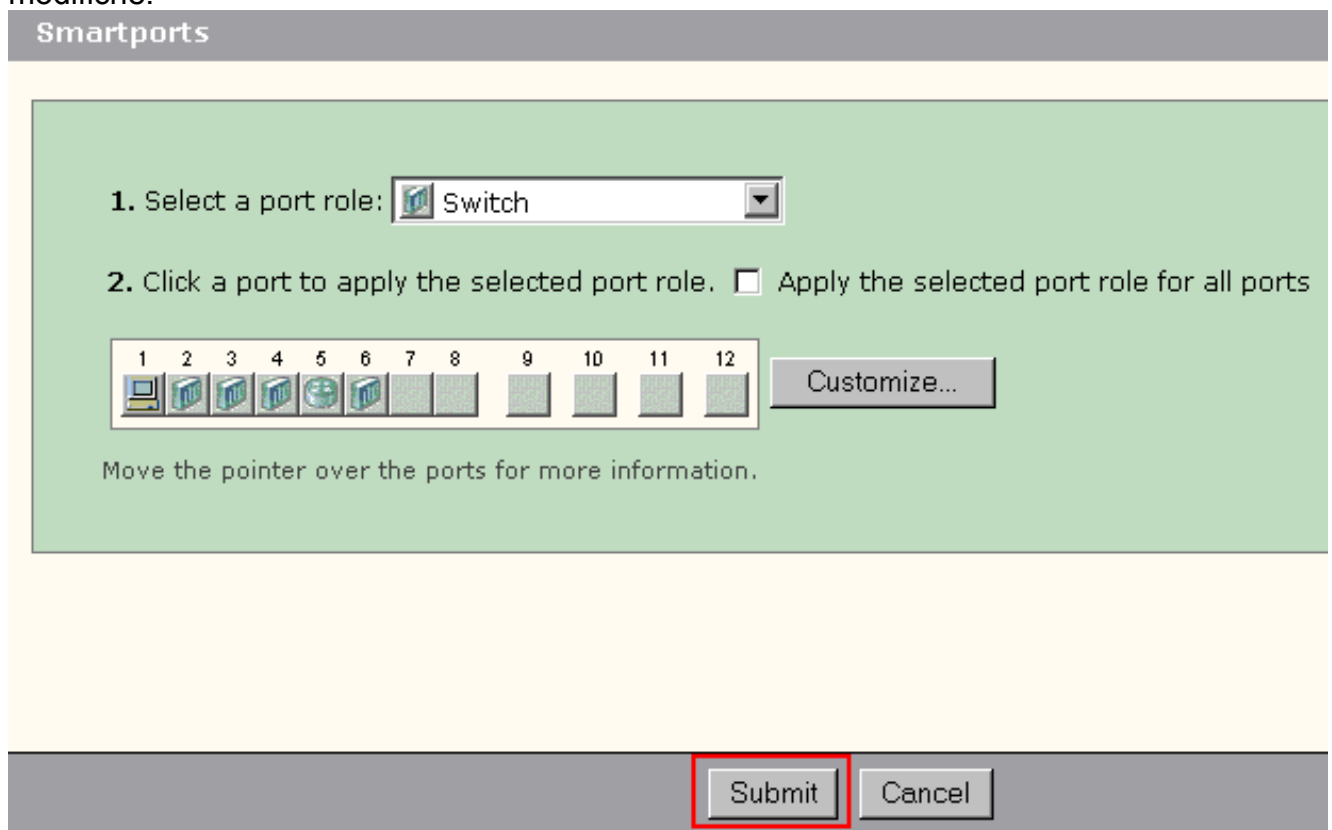
porta.

2. Fare clic sulla porta. Sulla porta viene visualizzata l'icona del ruolo Smartports



selezionato.

3. Fare clic su **Invia** per salvare le modifiche.



Per rimuovere il ruolo Smartports applicato a una porta, completare la procedura seguente:

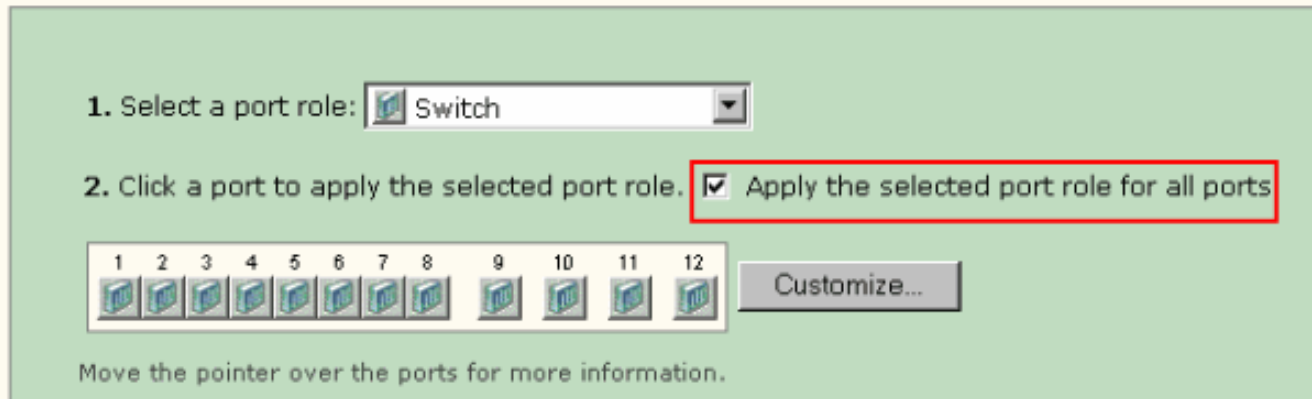
1. Scegliere **Altro** dall'elenco Selezionare un ruolo porta.
2. Fare clic sulla porta. Sulla porta viene visualizzata l'icona Altro.
3. Fare clic su **Invia** per salvare le modifiche.

### [Applicazione di un ruolo Smartports a tutte le porte](#)

Completare la procedura seguente per applicare il ruolo Smartports selezionato a tutte le porte:

1. Scegliere un ruolo Smartports dall'elenco Selezionare un ruolo porta.
2. Selezionare **Applica il ruolo porta selezionato a tutte le porte**. Sulle porte viene visualizzata l'icona del ruolo Smartports selezionato.

## Smartports



3. Completare questi passaggi per le porte che non devono essere applicate con il ruolo porta selezionato: Scegliere un altro ruolo Smartports dall'elenco Selezionare un ruolo porta. Fare clic sulla porta. Sulla porta viene visualizzata l'icona del ruolo Smartports selezionato.
4. Fare clic su **Invia** per salvare le modifiche.

Completare la procedura seguente per rimuovere il ruolo Smartports applicato a tutte le porte:

1. Scegliere **Altro** dall'elenco Selezionare un ruolo porta.
2. Selezionare **Applica il ruolo porta selezionato per tutte le porte**. Sulle porte viene visualizzata l'icona Altro.
3. Fare clic su **Invia** per salvare le modifiche.

## Creazione/eliminazione di VLAN

### Tipi di VLAN

Lo switch viene fornito con una VLAN predefinita a cui inizialmente tutte le porte dello switch appartengono. Lo switch supporta un massimo di 32 VLAN, inclusa la VLAN predefinita. L'utilizzo esclusivo della VLAN predefinita potrebbe essere sufficiente in base alle dimensioni e ai requisiti della rete. Prima di creare le VLAN, si consiglia di determinare le esigenze della VLAN.

**Nota:** gli switch Cisco Catalyst serie 5500 funzionano in modalità VTP trasparente. La creazione, la modifica o l'eliminazione di VLAN eseguita su questo switch non influisce sugli altri switch del dominio.

A seconda del tipo di dispositivo collegato alla porta dello switch:

- Una porta dello switch applicata con uno di questi ruoli della porta può appartenere solo a una VLAN di accesso: Desktop IP Phone e desktop Stampante Server Guest Other (Altro) La VLAN di accesso fornisce al dispositivo collegato l'accesso specifico progettato per quella VLAN.
- Una porta dello switch con uno di questi ruoli può inviare e ricevere traffico per tutte le VLAN configurate sullo switch, una delle quali può essere identificata come VLAN nativa: Switch Router Access Point Su questa porta, si presume che il traffico ricevuto o inviato senza la VLAN identificata in modo esplicito appartenga alla VLAN nativa. La porta dello switch e la porta del dispositivo collegato devono trovarsi sulla stessa VLAN nativa.

**Nota:** selezionare **Configura > Smartports > Personalizza** in Gestione dispositivi per visualizzare i ruoli della porta e le VLAN associate.

Port	Role	Native VLAN	Access VLAN	Voice VLAN	Server Type
Fa5	Desktop		default-1		
Fa6	Switch	default-1			
Fa7	Router	default-1			
Fa8	IP Phone+Desktop		default-1	none	
Fa9	Access Point	default-1			
Fa10	Server		default-1		Business
Fa11	Printer		default-1		
Fa12	Guest		default-1		

Done Cancel

Se la rete richiede la separazione del traffico voce o guest, è necessario creare altre VLAN. Se si creano altre VLAN sullo switch con IP Phone+Desktop e porte vocali Smart, è necessario creare anche le seguenti VLAN:

- **Cisco-Guest:** la VLAN a cui devono essere assegnate tutte le porte applicate con il ruolo di porta guest. Questa VLAN garantisce che tutto il traffico di ospiti e visitatori sia separato dal resto del traffico e delle risorse di rete. Le porte con ruoli **Guest** Smartport devono essere assegnate a questa VLAN.
- **Cisco-Voice:** la VLAN a cui devono essere assegnate tutte le porte applicate con il ruolo porta IP Phone+Desktop. Questa VLAN garantisce che tutto il traffico vocale abbia una migliore QoS e non venga mischiato al traffico di dati. La VLAN vocale delle porte con ruoli **IP Phone+Desktop** Smartport deve essere assegnata a questa VLAN.

Usare la finestra VLAN per creare ed eliminare le VLAN. Per visualizzare questa finestra, selezionare **Configure > VLAN** dal menu Device Manager.

1. Per creare una VLAN, effettuare i seguenti passaggi:
2. Fare clic su **Create** (Crea) nella finestra VLAN.

VLANs

Name	ID	Delete
default	1	<input type="checkbox"/>

3. Immettere il nome e l'ID della VLAN.

4. Selezionate **Fatto**  
(Done).

VLAN: Create

VLAN Name:

VLAN ID:

5. Ripetere i passaggi da 1 a 3 fino a creare le VLAN necessarie.

6. Fare clic su **Invia** per salvare le  
modifiche.

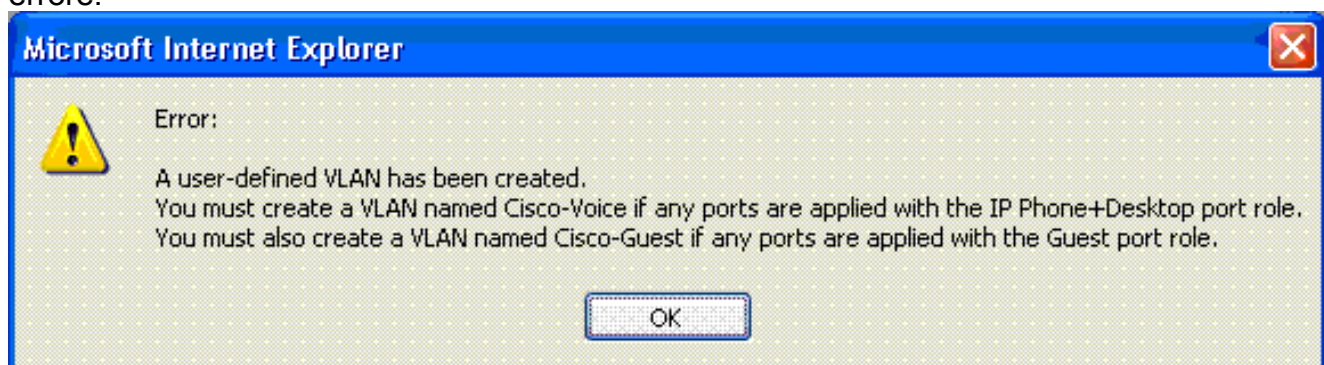
VLANs

Name ▲	ID	<input type="checkbox"/> Delete
Cisco-Guest	40	<input type="checkbox"/>
Cisco-Voice	3	<input type="checkbox"/>
VLAN2	2	<input type="checkbox"/>
default	1	<input type="checkbox"/>

Create Advanced

Submit Cancel

**Nota:** se si hanno porte con il ruolo IP Phone+Desktop, è necessario creare la VLAN Cisco-Voice. Se si hanno porte con ruolo porta guest, è necessario creare la VLAN Cisco-Guest. Se si creano VLAN senza VLAN Cisco-Voice e Cisco-Guest e si fa clic su **Submit**, viene visualizzato questo messaggio di errore.



Per eliminare le VLAN, attenersi alla procedura seguente:

1. Selezionare la casella di controllo nella parte superiore della colonna Delete per selezionare tutte le VLAN o selezionare la casella di controllo per una o più VLAN specifiche.



Name ▲	ID	Delete
Cisco-Guest	40	<input type="checkbox"/>
Cisco-Voice	3	<input type="checkbox"/>
VLAN2	2	<input type="checkbox"/>
VLAN50	50	<input checked="" type="checkbox"/>
default	1	<input type="checkbox"/>

2. Fare clic su **Invia** per salvare le modifiche. Fare clic su **OK** nella finestra a comparsa di conferma dell'eliminazione della VLAN.

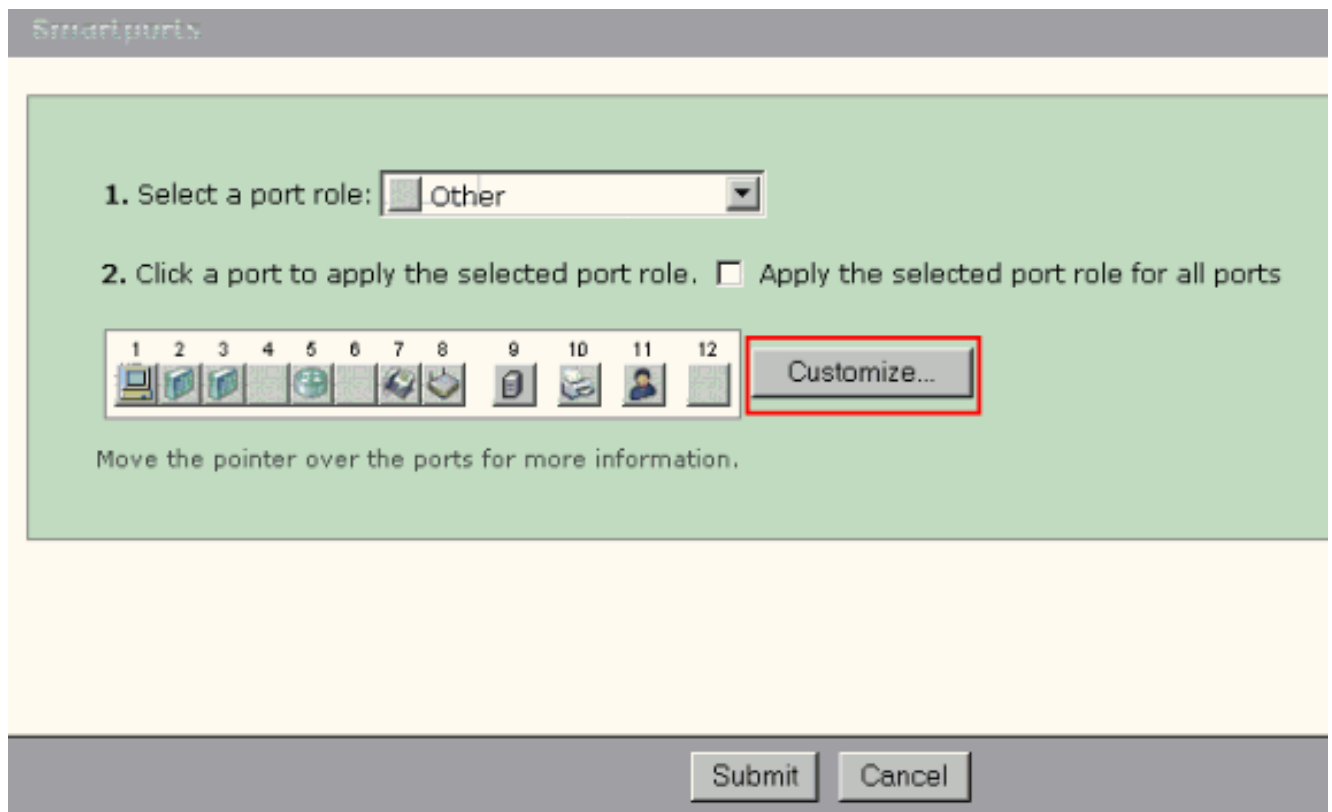
## [Modifica dell'appartenenza della VLAN](#)

È possibile modificare le appartenenze specifiche della VLAN per le porte che fanno parte dei seguenti ruoli Smartport:

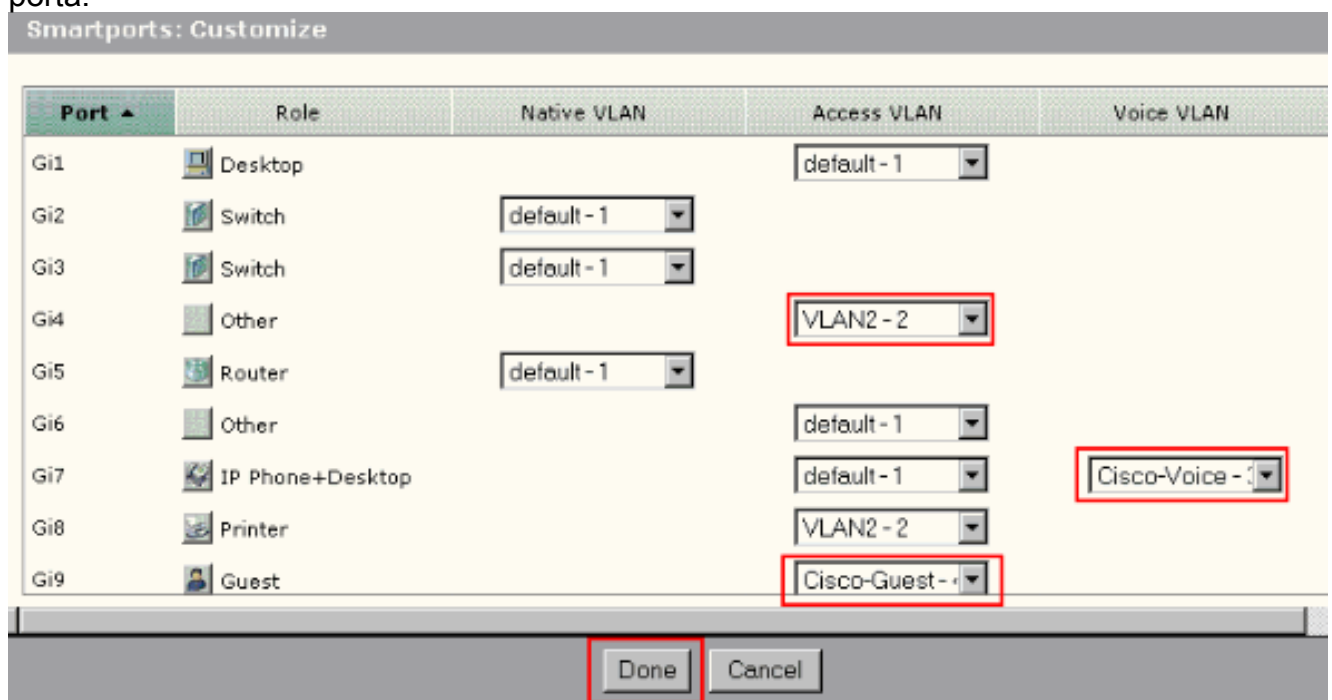
- **VLAN nativa:** switch, router e punto di accesso
- **Accesso alla VLAN:** desktop, IP Phone+desktop, server, stampante, guest e altro **Nota:** l'accesso alla VLAN per il ruolo di guest deve essere una VLAN Cisco-Guest.
- **Voice VLAN:** IP Phone+Desktop. Voice VLAN deve essere solo la VLAN Cisco-Voice.

Per assegnare le porte alle VLAN, usare la finestra Smartports Customize. Selezionare **Configura > Smartports** dal menu Gestione periferiche per visualizzare questa finestra.

1. Fare clic su **Personalizza** nella finestra Smartports.



2. Selezionare le VLAN appropriate per ciascuna porta.



3. Selezionate **Fatto (Done)**.
4. Fare clic su **Invia** per salvare le modifiche.

## [Configura EtherChannel](#)

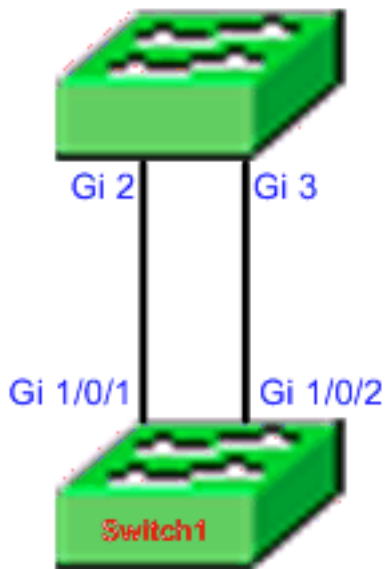
EtherChannel è un gruppo di due o più porte dello switch Fast Ethernet o Gigabit Ethernet incluse in un singolo collegamento logico che crea un collegamento con larghezza di banda più elevata tra due switch. Lo switch supporta fino a sei canali EtherChannel.

Tutte le porte in EtherChannel devono avere le stesse caratteristiche:

- Tutte le porte sono 10/100 o tutte 10/100/1000. Non è possibile raggruppare una combinazione di porte 10/100 e 10/100/1000 in un EtherChannel.
- Tutte le porte hanno le stesse impostazioni di velocità e modalità duplex.
- A tutte le porte viene applicato il ruolo porta switch Smartports e appartengono alla stessa VLAN.

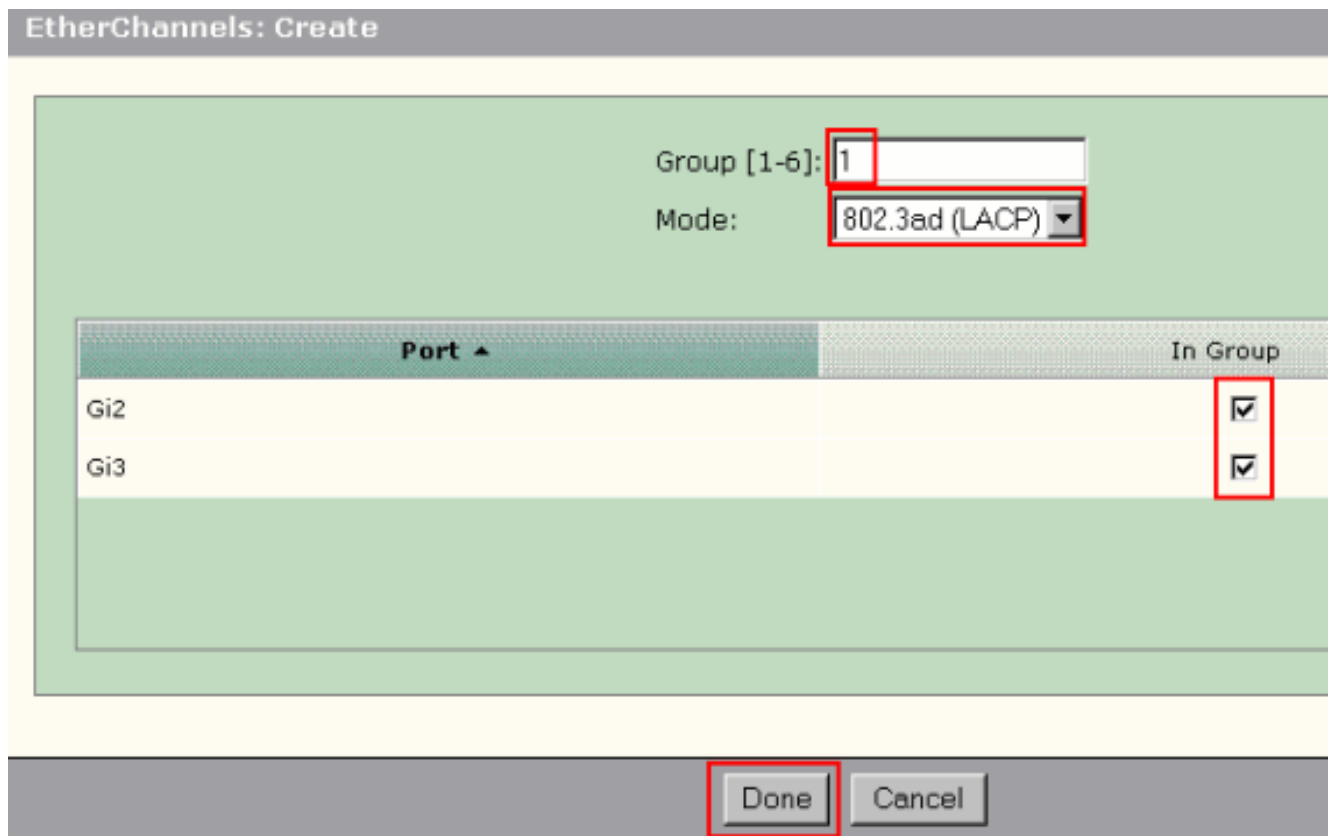
Completare questa procedura per creare EtherChannel tra un Cisco Catalyst Express 500 e un altro switch:

### Cisco Catalyst Express CE500G-12TC Switch



### Cisco Catalyst 3750 Series Switch

1. Da Gestione dispositivi dello switch Cisco Catalyst Express 500, selezionare **Configure > EtherChannels** per visualizzare la finestra EtherChannels.
2. Fare clic su **Crea**.
3. Immettere l'ID del gruppo di canali.
4. Scegliere il Protocollo canale (modalità) per l'elenco Modalità. **Nota:** lo switch Catalyst Express 500 supporta due modalità denominate LACP e Static. Configurare lo switch remoto in base alla modalità scelta.
5. Selezionare le caselle di controllo corrispondenti alle porte che devono far parte del canale.
6. Fare clic su **Fine**, quindi su **Invia** per salvare le modifiche.



7. Se è stato scelto il protocollo LACP per negoziare il canale, configurare lo switch remoto come mostrato in questo output:

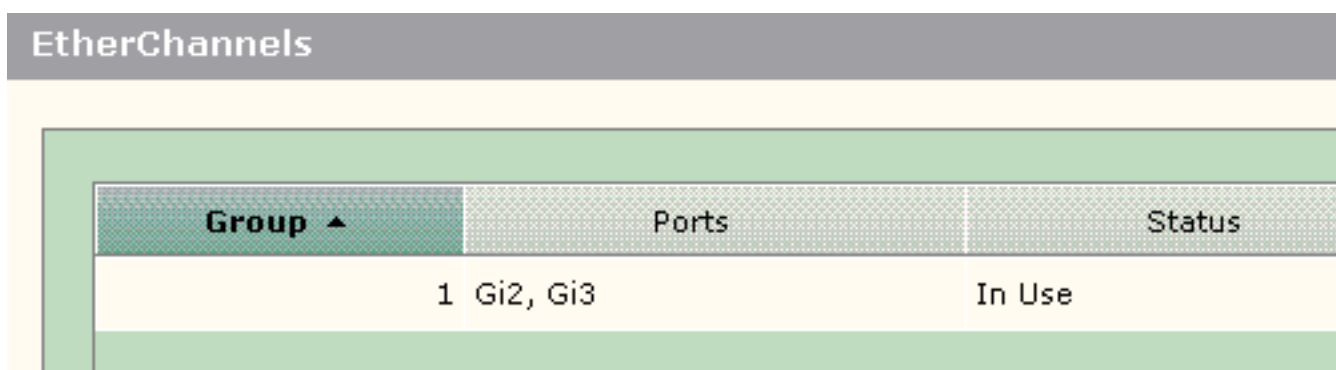
```
Switch1(config)#interface gi1/0/1
Switch1(config-if)#channel-group 1 mode active
Switch1(config-if)#interface gi1/0/2
Switch1(config-if)#channel-group 1 mode active
```

Se si sceglie di configurare il canale in modo statico, configurare lo switch remoto come mostrato nell'output:

```
Switch1(config)#interface gi1/0/1
Switch1(config-if)#channel-group 1 mode on
Switch1(config-if)#interface gi1/0/2
Switch1(config-if)#channel-group 1 mode on
```

## Verifica

Aprire la finestra **Configure > EtherChannels** per verificare lo stato di EtherChannel creato. Lo stato deve essere visualizzato come 'In uso'. In caso contrario, è possibile eseguire la diagnostica sulle porte per determinare il problema.



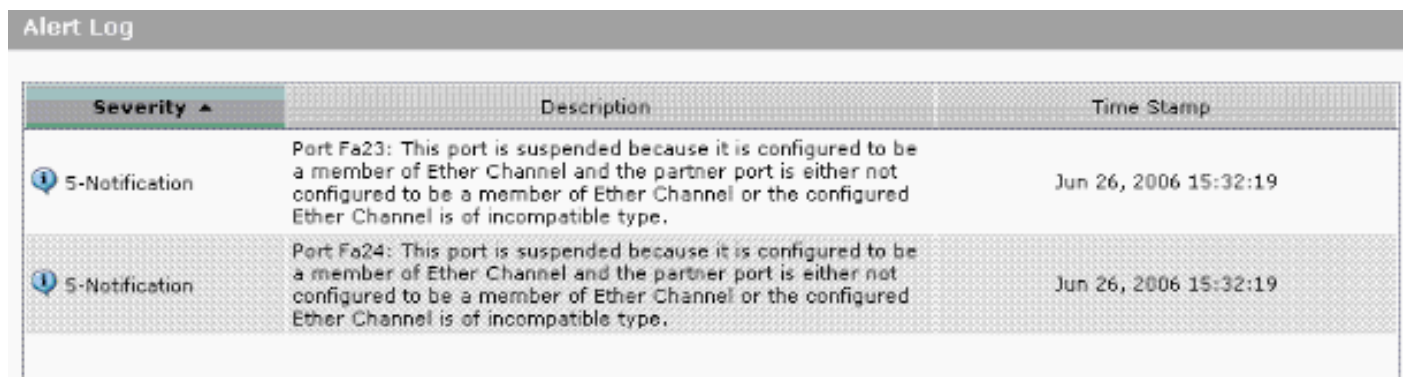
Eseguire il comando **show etherchannel summary** nello switch Cisco 3750 per verificare lo stato della configurazione EtherChannel. Il campo Protocollo nell'output visualizza LACP se viene utilizzato per negoziare il canale, vuoto o in altro modo.

```
Switch#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators:          1
```

```
Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SU)         LACP     Gi1/0/1(P) Gi1/0/2(P)
```

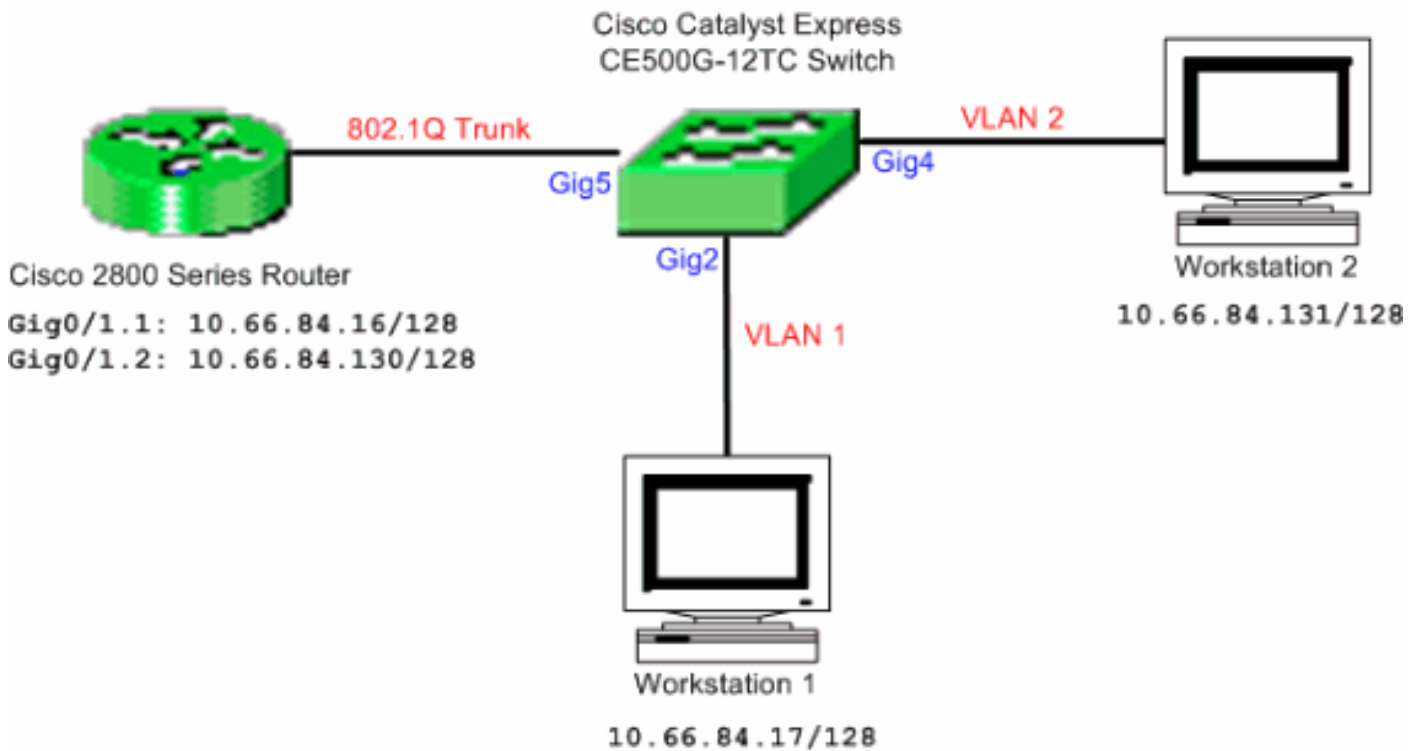
Inoltre, è possibile visualizzare il log dello switch Catalyst 5500 da **Monitor > Alert Log** in Gestione dispositivi. In questo esempio viene mostrato il messaggio di errore EtherChannel causato dalla configurazione errata di EtherChannel sullo switch remoto.



Severity ▲	Description	Time Stamp
5-Notification	Port Fa23: This port is suspended because it is configured to be a member of Ether Channel and the partner port is either not configured to be a member of Ether Channel or the configured Ether Channel is of incompatible type.	Jun 26, 2006 15:32:19
5-Notification	Port Fa24: This port is suspended because it is configured to be a member of Ether Channel and the partner port is either not configured to be a member of Ether Channel or the configured Ether Channel is of incompatible type.	Jun 26, 2006 15:32:19

## [Configurazione del routing tra VLAN con un router Cisco](#)

Esempio di rete



**Nota:** la configurazione di esempio usa il router Cisco serie 2800. Può essere sostituito con qualsiasi router Cisco che supporti il trunking IEEE 802.1Q.

Per configurare il routing tra VLAN con un router Cisco, attenersi alla procedura seguente:

1. Completare la procedura seguente per configurare lo switch Cisco Catalyst Express 500: Applicare il ruolo Smartport del desktop alle porte Gig2 e Gig4. Per la procedura di configurazione, vedere la sezione [Applicazione dei ruoli Smartport alle porte](#) di questo documento. Applicare il ruolo Smartport del router alla porta Gig5. Applicare gli ID VLAN appropriati alle porte. Assegnare la VLAN 1 come VLAN di accesso per la porta Gig2. Assegnare la VLAN 2 come VLAN di accesso per la porta Gig4. Assegnare la VLAN 1 come VLAN nativa per la porta Gig5. Per la procedura di configurazione, vedere la sezione [Modifica dell'appartenenza della VLAN](#) di questo documento.

2. Configurare il router Cisco serie 2800:

```
Router(config)#interface GigabitEthernet0/1.1
Router(config-subif)#encapsulation dot1q 1 native
Router(config-subif)#ip address 10.66.84.16 255.255.255.128
Router(config-subif)#interface GigabitEthernet0/1.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 10.66.84.130 255.255.255.128
```

## Verifica

Selezionare **Monitor > Port Status** (Stato porta) in Device Manager per verificare lo stato del trunk della porta dello switch sullo switch Catalyst Express 500.

## Port Status

Port	Description	Status	VLAN	Speed	Duplex	PoE	Auto-MDIX
Fa2		●	1			Off	On
Fa3		●	1			Off	On
Fa4		●	1			Off	On
Fa5		●	1			N/A	On
Fa6		●	1			N/A	On
Fa7		●	trunk	100	full	N/A	On
Fa8		●	1			N/A	On

Verificare che il ping tra la Workstation 1 e la Workstation 2 abbia esito positivo.

```
C:\>ping 10.66.84.131
```

```
Pinging 10.66.84.131 with 32 bytes of data:
```

```
Reply from 10.66.84.131: bytes=32 time<10ms TTL=128
Reply from 10.66.84.131: bytes=32 time<10ms TTL=128
Reply from 10.66.84.131: bytes=32 time<10ms TTL=128
Reply from 10.66.84.131: bytes=32 time<10ms TTL=128
```

```
Ping statistics for 10.66.84.131:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Eseguire una traccia per verificare il percorso utilizzato per la comunicazione tra Workstation 1 e Workstation 2.

```
C:\>tracert 10.66.84.131
```

```
Tracing route to 10.66.84.131 over a maximum of 30 hops
```

```
 0  <10 ms  <10 ms  <10 ms  10.66.84.16
 1  <10 ms  <10 ms  <10 ms  10.66.84.131
```

```
Trace complete.
```

## [Configurazione di SPAN \(Switched Port Analyzer\)](#)

La funzionalità SPAN (Switched Port Analyzer), chiamata anche mirroring delle porte o monitoraggio delle porte, seleziona il traffico di rete per l'analisi da parte di un analizzatore di rete. L'analizzatore di rete può essere un dispositivo Cisco SwitchProbe o un'altra sonda RMON (monitoraggio da remoto). Lo switch supporta solo lo SPAN locale e non supporta lo SPAN remoto.

La porta di destinazione deve essere configurata con il ruolo Smartport di diagnostica. A tale scopo, è possibile usare solo il software Cisco Network Assistant. Per configurare lo switch Catalyst Express 500 in modo da monitorare il traffico, consultare il documento [SPAN sul Catalyst Express 500](#).

## [Ripristino delle impostazioni predefinite dello switch Catalyst Express 500](#)

Se si dispone della connettività a Gestione dispositivi dello switch e si desidera ripristinare le impostazioni predefinite dello switch e mantenere il software di sistema Cisco IOS corrente, fare riferimento alla sezione [Ripristino del valore predefinito dello switch con Gestione dispositivi](#) nel documento [Ripristino dei valori predefiniti sugli switch Catalyst Express serie 500](#).

Se non si dispone della connettività a Gestione dispositivi dello switch e si desidera ripristinare lo switch ai valori predefiniti, fare riferimento alla sezione [Ripristino dello switch quando Gestione dispositivi non è disponibile](#) nel documento [Ripristino dei valori predefiniti sugli switch Catalyst serie 500](#).

Per ulteriori informazioni sulla procedura di ripristino, consultare la sezione [Ripristino del software dello switch](#) nel [Manuale dell'utente degli switch Catalyst Express 500 - Risoluzione dei problemi](#).

## [Verifica](#)

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## [Risoluzione dei problemi](#)

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## [Informazioni correlate](#)

- [Guida introduttiva agli switch Catalyst Express 500](#)
- [Guida per l'utente degli switch Catalyst Express 500](#)
- [Informazioni sul bilanciamento del carico EtherChannel e sulla ridondanza negli switch Catalyst](#)
- [Configurazione del routing tra VLAN e trunking ISL/802.1Q su uno switch Catalyst 2900XL/3500XL/2950 con router esterno](#)
- [Switch - Supporto dei prodotti](#)
- [Supporto della tecnologia di switching LAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)