

Trunking tra switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000 con incapsulamento 802.1Q con software Cisco CatOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Che cos'è un trunk?](#)

[Caratteristiche di base del trunking 802.1Q](#)

[Meccanismo di tag](#)

[Considerazioni sullo Spanning Tree](#)

[Implementazione Cisco](#)

[Configurazione dei trunk 802.1Q](#)

[Requisiti hardware/software](#)

[Modalità DTP](#)

[Esempio dettagliato](#)

[Errori comuni](#)

[VLAN native diverse](#)

[Domini VTP diversi](#)

[Errore durante un tentativo di eliminare VLAN dell'intervallo esteso da una porta trunk](#)

[Modalità trunking non compatibile con il tipo di incapsulamento](#)

[Comandi utilizzati nel documento](#)

[Riepilogo comandi](#)

[Informazioni correlate](#)

Introduzione

Questo documento introduce il concetto di trunking tra due switch Ethernet e si concentra sullo standard di trunking IEEE 802.1Q. Dopo una breve descrizione del meccanismo di trunking 802.1Q, il documento descrive l'implementazione sugli switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000. Viene fornito un esempio completo, insieme ad alcuni errori comuni relativi alla configurazione del trunking 802.1Q con l'uso del software di sistema Catalyst OS (CatOS). Per esempi di trunking 802.1Q con il software di sistema Cisco IOS®, fare riferimento alla [configurazione del trunking 802.1Q tra uno switch Catalyst 3550/3560/3750 e gli switch Catalyst con software Cisco IOS](#).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Convenzioni

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

Che cos'è un trunk?

Nella terminologia Cisco, un trunk è un collegamento point-to-point che porta diverse VLAN. Lo scopo di un trunk è salvare le porte quando si crea un collegamento tra due dispositivi che implementano le VLAN, in genere due switch. Nel diagramma riportato di seguito vengono mostrate due VLAN che si desidera rendere disponibili su due switch, Sa e Sb. Il primo metodo facile da implementare è la creazione di due collegamenti fisici tra i dispositivi. I collegamenti fisici trasportano ciascuno il traffico di una VLAN:



Ovviamente, questa soluzione non è scalabile. Per aggiungere una terza VLAN, è necessario aggiungere altre due porte. Questo progetto è inefficiente anche in termini di ripartizione del carico; il traffico su alcune VLAN potrebbe non giustificare un collegamento dedicato. Un trunk raggruppa i collegamenti virtuali su un collegamento fisico, come illustrato nel diagramma seguente:



In questo modo, l'unico collegamento fisico tra i due switch può trasmettere il traffico di tutte le VLAN. A tale scopo, ogni frame inviato sul collegamento viene contrassegnato dalla scheda Sa in modo che Sb conosca la VLAN a cui appartiene. Esistono diversi schemi di tagging. I più comuni per i segmenti Ethernet sono:

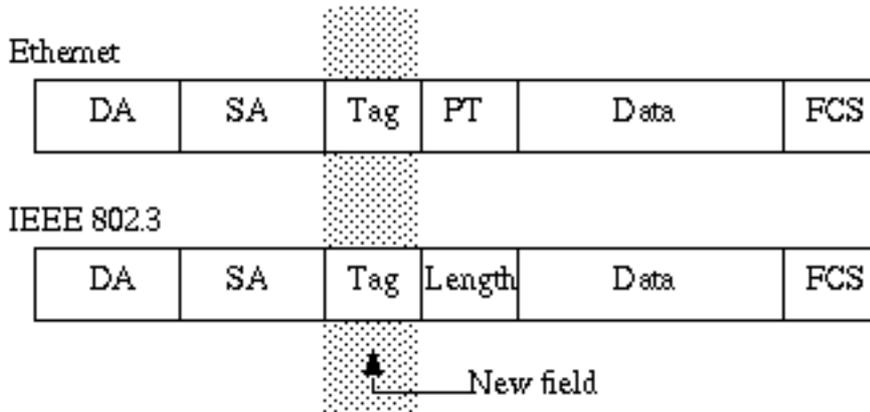
- ISL (Inter-Switch Link) (protocollo ISL originale di proprietà di Cisco)
- 802.1Q (lo standard IEEE su cui si concentra questo documento)

Caratteristiche di base del trunking 802.1Q

Meccanismo di tag

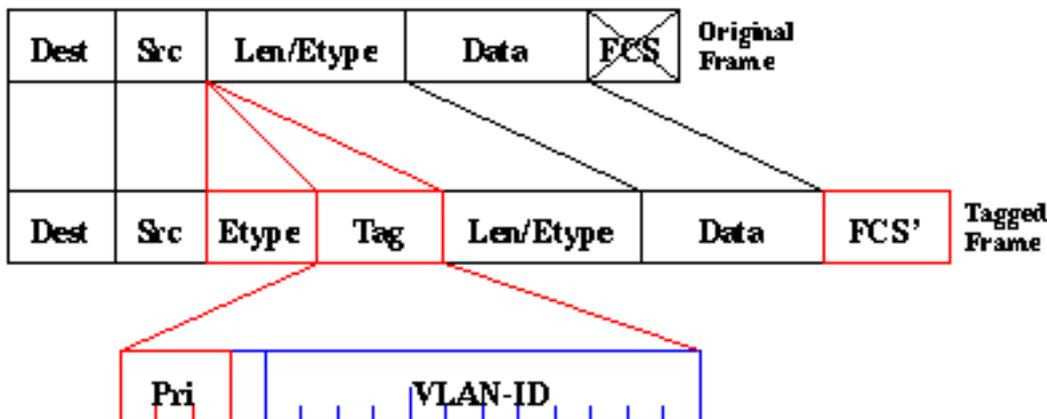
802.1Q utilizza un meccanismo di tag interno. Interno significa che un tag viene inserito all'interno del frame:

Nota: con ISL, il frame è incapsulato.



Nota: su un trunk 802.1Q, una VLAN NON ha tag. Questa VLAN, denominata VLAN nativa, deve essere configurata allo stesso modo su ciascun lato del trunk. In questo modo, è possibile dedurre a quale VLAN appartiene un frame quando si riceve un frame senza tag.

Il meccanismo di marcatura implica una modifica del telaio; il dispositivo trunking inserisce un tag di 4 byte e ricalcola la sequenza di controllo del fotogramma (FCS):

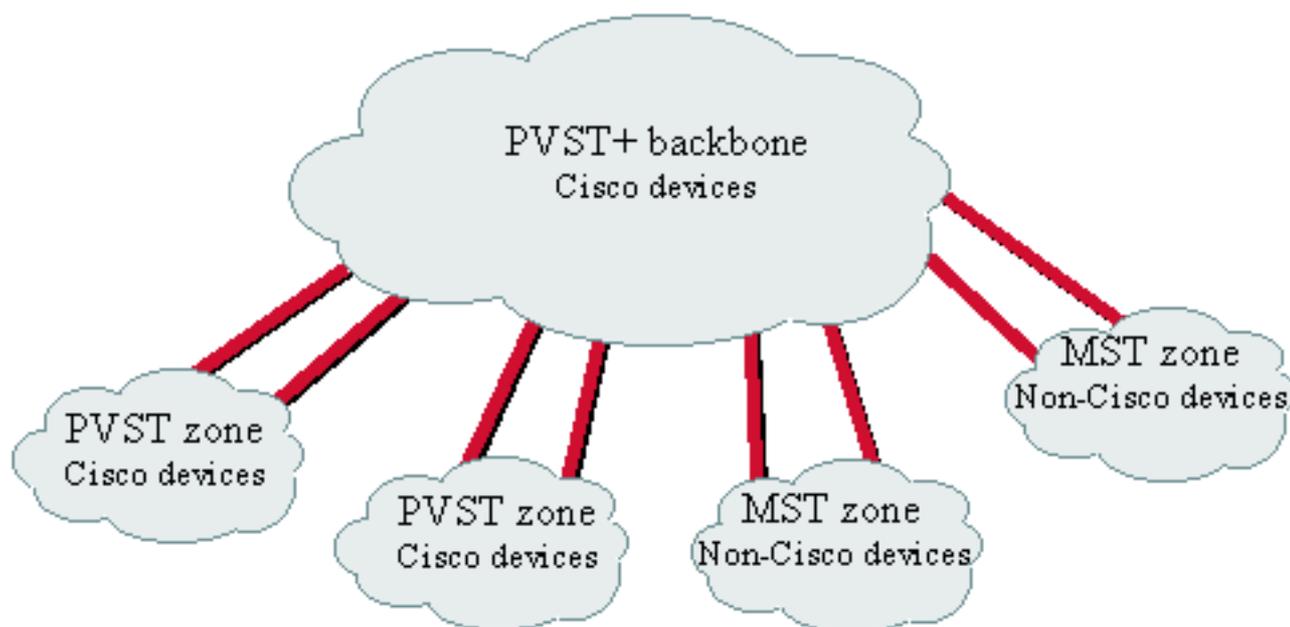


Il campo EtherType che identifica il frame 802.1Q è 0x8100. Oltre all'ID VLAN a 12 bit, 3 bit sono riservati per il tagging di priorità IEEE 802.1p.

Nota: l'inserimento di un tag in un frame che ha già le dimensioni Ethernet massime crea un frame di 1522 byte che può essere considerato un "gigante del bambino" dall'apparecchiatura ricevente. Il comitato IEEE 802.3 sta estendendo la dimensione massima standard del frame per affrontare questo problema.

Considerazioni sullo Spanning Tree

Lo standard 802.1Q è molto di più di un semplice meccanismo di tagging. Definisce anche un'istanza unica dello Spanning Tree che viene eseguita sulla VLAN nativa per tutte le VLAN nella rete. Una rete MST (Mono Spanning Tree) di questo tipo manca di flessibilità rispetto a una rete PVST (Per VLAN Spanning Tree) che esegue un'istanza del protocollo STP (Spanning Tree Protocol) per VLAN. Cisco ha sviluppato PVST+ per consentire l'esecuzione di diverse istanze STP (anche su una rete 802.1Q) tramite un meccanismo di tunneling. Anche se al di fuori dell'ambito di questo documento, è possibile descrivere brevemente l'utilizzo di un dispositivo Cisco per connettere una zona MST (in genere la rete basata sullo standard 802.1Q di un altro fornitore) a una zona PVST (in genere una rete basata su Cisco ISL). Per ottenere questo risultato, non è necessario immettere una configurazione specifica. In teoria, un ambiente misto dovrebbe avere il seguente aspetto:



No direct trunk can be established between a MST and PVST zone.
There has to be a PVST+ zone in between.

Implementazione Cisco

Nell'implementazione corrente, i dispositivi Cisco supportano solo i numeri VLAN fino a 1005. Questa restrizione, introdotta per far corrispondere il numero di VLAN disponibili con ISL, è consentita dallo standard 802.1Q. Cisco ha implementato una funzione di mappatura VLAN in CatOS 5.1 per semplificare l'interoperabilità con altri dispositivi del fornitore, ma raramente è necessaria.

Nota: per informazioni sulla funzione di mappatura VLAN, consultare il documento sulla [configurazione](#) delle VLAN.

Cisco ha inoltre adattato il protocollo DISL (Dynamic ISL) e lo ha convertito in DTP (Dynamic Trunking Protocol). DISL può negoziare il trunking ISL su un collegamento tra due dispositivi; il DTP può inoltre negoziare il tipo di incapsulamento trunking (802.1Q o ISL) che verrà utilizzato. Questa funzionalità è interessante in quanto alcuni dispositivi Cisco supportano solo ISL o 802.1Q, mentre altri possono eseguire entrambi.

Nell'implementazione di Cisco, un trunk è un collegamento point-to-point, anche se è possibile

utilizzare l'incapsulamento 802.1Q su un segmento Ethernet condiviso da più di due dispositivi. Tale configurazione è raramente necessaria, ma è ancora possibile con la disabilitazione della negoziazione DTP.

Configurazione dei trunk 802.1Q

Requisiti hardware/software

Dal punto di vista del software, la prima apparizione dell'incapsulamento 802.1Q è stata con il software CatOS 4.1. In questa versione, la configurazione del trunking doveva essere hardcoded; Il DTP è apparso solo con CatOS 4.2. Vedere la sezione [Modalità DTP](#) di questo documento.

Non tutte le porte Catalyst supportano l'incapsulamento 802.1Q. Al momento, mentre gli switch Catalyst 4500/4000 supportano solo 802.1Q, le porte della serie Catalyst 6500/6000 sono in grado di utilizzare l'incapsulamento 802.1Q o ISL. A seconda del modulo, le porte Catalyst 5500/5000 compatibili con il trunk possono usare l'incapsulamento 802.1Q, l'incapsulamento ISL o entrambi. Il modo migliore per verificare questa condizione è tramite il comando [show port capabilities](#). La capacità di trunking è esplicitamente indicata:

```
Sa> (enable) show port capabilities 1/1
Model                WS-X5530
Port                 1/1
Type                 1000BaseSX
Speed                1000
Duplex                full
Trunk encap type     802.1Q,ISL
Trunk mode            on,off,desirable,auto,nonegotiate
Channel              no
Broadcast suppression percentage(0-100)
Flow control          receive-(off,on,desired),send-(off,on,desired)
Security              no
Membership            static
Fast start            yes
Rewrite               no
```

Modalità DTP

Quando si configura una porta per il trunking, è possibile impostare due parametri: la modalità trunking e il tipo di incapsulamento (se il DTP è supportato su quella porta).

- La **modalità trunking** definisce il modo in cui la porta negozia la configurazione di un trunk con la relativa porta peer. Di seguito sono elencate le possibili impostazioni: Prestare attenzione affinché alcune modalità (*on*, *nonegotiate*, *off*) specifichino esplicitamente lo stato in cui la porta terminerà. Una configurazione errata può portare a uno stato pericoloso e incoerente in cui un lato è trunking e l'altro no. Una porta *accesa*, *automatica*, o *desiderata* invia periodicamente frame DTP. Una porta trunking in modalità *auto* o *desiderabile* torna a non trunking se non riceve un aggiornamento DTP dal router adiacente entro 5 minuti. **Nota:** se si esegue il software CatOS 4.1, è necessario disabilitare qualsiasi forma di negoziazione utilizzando la modalità *off* o *nonegotiate* quando si configura il trunking 802.1Q.
- Il **tipo di incapsulamento** permette di specificare se usare 802.1Q o ISL durante la configurazione del trunk. Naturalmente, il parametro è rilevante solo se il modulo utilizzato è in grado di utilizzare entrambi. Il parametro può avere tre valori diversi:

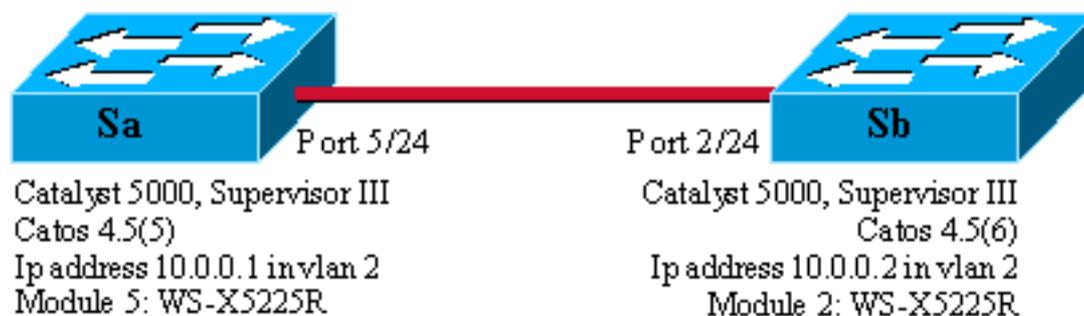
Per un elenco di tutte le possibili configurazioni, consultare la sezione [Risultati di possibili configurazioni di Fast Ethernet e Gigabit Ethernet Trunk](#) in [Configurazione dei trunk VLAN sulle porte Fast Ethernet e Gigabit Ethernet](#).

Nota: non verrà eseguita alcuna negoziazione tra due switch in domini VLAN Trunk Protocol (VTP) diversi. Fare riferimento alla sezione sulla [configurazione del VTP](#).

Esempio dettagliato

Esempio di rete

Questo esempio si basa su una configurazione lab molto semplice che coinvolge due switch Catalyst 5500/5000 collegati tra loro tramite porte compatibili con il trunk. Per interconnettere due switch, è necessario un [cavo crossover](#).



Configurazione minima di un trunk 802.1Q con test di connettività

Attenersi alla seguente procedura:

1. Verificare che lo stato delle porte sia attivo ma non trunking. Collegare un terminale alla console degli switch. Se necessario, consultare il documento sul [collegamento di un terminale alla porta console sugli switch Catalyst](#). Verificare innanzitutto lo stato della porta coinvolta nell'installazione. Utilizzare il comando [show port 5/24](#) su Sa ([show port 2/24](#) su Sb) e verificare che lo stato sia connected (connesso):

```
Sa> (enable) show port 5/24
Port Name Status Vlan Level Duplex Speed Type
-----
5/24 connected 1 normal a-full a-100 10/100BaseTX
!--- Output suppressed.
```

Il valore predefinito per il tipo di porta è. È stata introdotta durante la negoziazione di un full duplex di 100 MB e viene assegnata alla VLAN 1. Usare il comando [show trunk 5/24](#) per verificare chiaramente che la porta non è trunking e dispone di una negoziazione automatica e incapsulamento della modalità predefinita.

```
Sa> (enable) show trunk 5/24
Port Mode Encapsulation Status Native vlan
-----
5/24 auto negotiate not-trunking 1
!--- Output suppressed.
```

2. Impostare un indirizzo IP sulle interfacce di gestione sc0. Per assegnare un indirizzo IP ai due switch, usare il comando [set interface sc0 10.0.0.1](#) sullo switch Sa e il comando [set interface sc0 10.0.0.2](#) sullo switch Sb. Il comando [show interface](#) conferma che l'interfaccia di gestione

è ora impostata correttamente sulla VLAN predefinita 1:

```
Sa> (enable) set interface sc0 10.0.0.1  
Interface sc0 IP address set.
```

```
Sa> (enable) show interface  
sl0: flags=51<,POINTOPOINT,RUNNING>  
    slip 0.0.0.0 dest 0.0.0.0  
sc0: flags=63<UP,BROADCAST,RUNNING>  
    vlan 1 inet 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255  
Sa> (enable)
```

se il dispositivo Cisco restituisce i risultati di un comando **show interface**, è possibile usare [Output Interpreter](#) (solo utenti [registrati](#)) per visualizzare i potenziali errori e correggerli.

3. Verificare la connettività tra Sa e Sb. Eseguire il comando [ping 10.0.0.2](#) dallo switch Sa per verificare che sia possibile raggiungere lo switch Sb:

```
Sa> (enable) ping 10.0.0.2  
10.0.0.2 is alive  
Sa> (enable)
```

4. Configurare lo stesso dominio VTP su entrambi gli switch. A questo punto, assegnare lo stesso dominio VTP a entrambi gli switch. Come avete visto, avere lo stesso dominio VTP è obbligatorio per utilizzare la negoziazione DTP. Usare il comando [set vtp domain cisco](#) su entrambi gli switch per configurarli con il nome di dominio "cisco":

```
Sa> (enable) set vtp domain cisco  
VTP domain cisco modified  
Sa> (enable)
```

5. Creare una VLAN 2 in ciascuno switch. Usare il comando [set vlan 2](#) su entrambi gli switch per creare la VLAN 2. Se gli switch erano già collegati da un trunk, sarà necessario usare il comando solo su uno switch, e l'altro switch lo imparerà automaticamente tramite VTP. Poiché non si dispone ancora di un trunk, non vi è alcuna comunicazione VTP tra Sa e Sb:

```
Sa> (enable) set vlan 2  
Vlan 2 configuration successful  
Sa> (enable)
```

6. Modificare le interfacce di gestione in VLAN 2. A questo punto, l'interfaccia di gestione di entrambi gli switch viene spostata nella VLAN 2. In questo modo, si dimostra che non vi è alcuna comunicazione tra le schede Sa e Sb prima che venga stabilito un trunk. Utilizzare il comando [set interface sc0 2](#) su ciascuno switch per spostare l'interfaccia sc0 nella VLAN 2. Per verificare l'efficacia del comando, usare il comando [show interface](#):

```
Sa> (enable) set interface sc0 2  
Interface sc0 vlan set.  
Sa> (enable) show interface  
sl0: flags=51<UP,POINTOPOINT,RUNNING>  
    slip 0.0.0.0 dest 0.0.0.0  
sc0: flags=63<UP,BROADCAST,RUNNING>  
    vlan 2 inet 10.0.0.1 netmask 255.0.0.0 broadcast 10.255.255.255  
Sa> (enable)
```

7. Verificare se la connettività tra i due switch è interrotta. A questo punto, il comando [ping 10.0.0.2](#) su Sb ha esito negativo tra le VLAN 2 e la Sb, a dimostrazione che non è disponibile connettività tra gli switch:

```
Sa> (enable) ping 10.0.0.2  
no answer from 10.0.0.2  
Sa> (enable)
```

8. Controllare le funzionalità della porta. Prima di iniziare a configurare un trunk, è possibile verificare con il comando [show port capabilities](#) che entrambe le porte siano in grado di implementare il trunking 802.1Q:

```
Sa> (enable) show port capabilities 5/24  
Model                WS-X5225R  
Port                  5/24
```

```

Type                10/100BaseTX
Speed               auto,10,100
Duplex              half,full
Trunk encap type    802.1Q,ISL
Trunk mode          on,off,desirable,auto,nonegotiate
Channel             5/23-24,5/21-24
Broadcast suppression percentage(0-100)
Flow control        receive-(off,on),send-(off,on)
Security            yes
Membership          static,dynamic
Fast start          yes
Rewrite             yes
Sa> (enable)

```

9. Configurare l'incapsulamento del trunk in modo che sia 802.1Q. A questo punto, è necessario configurare il trunk su Sa. Nel passaggio 1 è stato rilevato che entrambe le porte si trovano nella modalità di trunking predefinita auto, negoziazione del tipo di incapsulamento. Una combinazione di auto-auto non porta un trunk su. Si tratta di un comportamento normale; ciascuna parte è disposta a diventare trunk, ma lo farà solo se il remoto lo richiede. Considerando la configurazione predefinita: È sufficiente modificare la modalità trunk in desiderata su un lato per portare il trunk su. Infatti, in modalità desiderabile, una porta notifica al proprio router adiacente che desidera passare alla modalità trunking. Quando il telecomando (in modalità automatica) passa al trunking, se richiesto, è sufficiente per sollevare il trunk. Se si configura l'incapsulamento dot1q su una sottointerfaccia, ciò significa che la VLAN non può essere riutilizzata nel sistema perché internamente, gli switch 6500 o 7600 allocano la VLAN e quindi fanno della sottointerfaccia l'unico membro. Non è quindi possibile avere una VLAN e provare a utilizzarla in una sottointerfaccia o viceversa. Per risolvere il problema, creare porte trunk anziché sottointerfacce e visualizzare la VLAN in questo modo su tutte le interfacce. Se sono necessarie sottointerfacce, le VLAN aggiunte nelle sottointerfacce non possono essere utilizzate in altre porte. È inoltre necessario specificare l'incapsulamento da utilizzare. Infatti, entrambe le porte sono compatibili con ISL e l'incapsulamento viene scelto per primo quando entrambe le estremità sono in modalità di negoziazione. La sintassi del comando è: **set trunk *module/port* [attivato] | disattivato | auspicabile | automatico | non negoziare] [intervallo_vlan] [isl | dot1q | negoziare]**. Eseguire il comando [set trunk 5/24 dot1q](#) desiderabile sullo switch Sa:

```

Sa> (enable) set trunk 5/24 dot1q desirable
Port(s) 5/24 trunk mode set to desirable.
Port(s) 5/24 trunk type set to dot1q.
1997 May 07 17:32:01 %DTP-5-TRUNKPORTON:Port 5/24 has become dot1q trunk
1997 May 07 17:32:02 %PAGP-5-PORTFROMSTP:Port 5/24 left bridge port 5/24
1997 May 07 17:32:13 %PAGP-5-PORTTOSTP:Port 5/24 joined bridge port 5/24

```

10. Verificare che il trunk sia attivo. Il log della console del comando precedente mostra chiaramente che la porta è stata spostata sul trunking, ma è possibile anche usare il comando [show trunk 5/24](#) su Sb e il comando [show trunk 2/24](#) per controllare. Potete vedere una sottile differenza tra i due output: La porta su Sa è in modalità desiderabile, mentre la porta Sb è in modalità automatica. Più interessante, l'incapsulamento è dot1q su Sa mentre è n-dot1q su Sb. In questo modo si dimostra che Sb ha negoziato il suo incapsulamento in dot1q. Se non si specifica un incapsulamento in Sa, entrambe le porte risulteranno incapsulate in n-isl:

```

Sa> (enable) show trunk 5/24

```

Port	Mode	Encapsulation	Status	Native vlan
5/24	desirable	dot1q	trunking	1

```

Port          Vlans allowed on trunk

```

```

-----
5/24      1-1005

Port      Vlans allowed and active in management domain
-----
5/24      1-2

Port      Vlans in spanning tree forwarding state and not pruned
-----
5/24      1-2
Sa> (enable)
Sb> (enable) show trunk 2/24
Port      Mode          Encapsulation  Status      Native vlan
-----
2/24      auto          n-dot1q        trunking    1
!--- Output suppressed.

```

se il dispositivo Cisco restituisce i risultati di un comando **show trunk**, è possibile usare [Output Interpreter](#) (solo utenti [registrati](#)) per visualizzare i potenziali errori e correggerli.

- Controllare la connettività. Per verificare che la VLAN 2 stia attraversando il trunk, è sufficiente eseguire il ping di Sb dal router Sa:

```

Sa> (enable) ping 10.0.0.2
10.0.0.2 is alive
Sa> (enable)

```

Impostazione della VLAN nativa

Attenersi alla seguente procedura:

- Usare il comando **set vlan**. Il comando [set vlan 2 5/24](#) viene usato per assegnare una porta a una VLAN specifica. Nel caso di una porta trunking, viene modificata la VLAN nativa in VLAN 2.
- Naturalmente, è necessario eseguire la stessa operazione su Sb con [set vlan 2/24](#):

```

Sa> (enable) set vlan 2 5/24
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
-----
2      5/24

```

```

Sa> (enable)

```

Prima di modificare la VLAN nativa su Sb, si è verificata un'incoerenza tra la configurazione Sa e la configurazione Sb. Le due estremità del trunk non hanno la stessa configurazione VLAN nativa. Di seguito vengono visualizzati alcuni messaggi di avviso sulla console secondaria. **Nota:** lo switch che segnala l'incoerenza può variare, a seconda di quale delle due è il bridge principale.

```

Sb> (enable) 2000 Dec 07 16:31:24 %SPANTREE-2-RX_1QPVIDERR: Rcvd
pvid_inc BPDU on 1Q port 2/24 vlan 1.
2000 Dec 07 16:31:24 %SPANTREE-2-TX_BLKPORTPVID: Block 2/24 on xmtting
vlan 2 for inc peer vlan.
2000 Dec 07 16:31:24 %SPANTREE-2-RX_BLKPORTPVID: Block 2/24 on rcving
vlan 1 for inc peer vlan 2.

```

```

Sb> (enable)
Sb> (enable) set vlan 2 2/24
VLAN 2 modified.
VLAN 1 modified.
VLAN  Mod/Ports
-----
2      2/24

```

```
Sb> (enable) 2000 Dec 07 16:31:46 %SPANTREE-2-PORTUNBLK: Unblock
previously inc port 2/24 on vlan 1.
2000 Dec 07 16:31:48 %SPANTREE-2-PORTUNBLK: Unblock previously inc
port 2/24 on vlan 2.
```

La mancata corrispondenza della VLAN nativa è stata corretta e tutto torna alla normalità.

- Controllate il risultato. A questo punto, è sufficiente controllare il risultato di questi comandi sul trunk con il comando [show trunk 5/24](#):

```
Sa> (enable) show trunk 5/24
Port      Mode      Encapsulation  Status      Native vlan
-----
5/24     desirable dot1q           trunking    2
<
```

[Specificare le VLAN consentite sul trunk](#)

Attenersi alla seguente procedura:

- Creare VLAN aggiuntive. Quando si crea un nuovo trunk, per impostazione predefinita vengono trasferite tutte le VLAN esistenti nella rete. Verrà spiegato come limitare l'elenco delle VLAN consentite su un trunk. Innanzitutto, occorre creare due VLAN aggiuntive (3 e 4). Ad esempio, è possibile usare il comando [set vlan 3](#) e il comando [set vlan 4](#) sulla VLAN per creare le VLAN aggiuntive. Il comando deve essere immesso su un solo switch; Il VTP propaga queste informazioni all'altro switch. **Nota:** questa parte della configurazione è assolutamente la stessa se si usa l'incapsulamento 802.1Q o ISL.

```
Sa> (enable) set vlan 3
Vlan 3 configuration successful
Sa> (enable) set vlan 4
Vlan 4 configuration successful
```

- Rimuovere le VLAN dal trunk. Il comando **clear trunk module/port vlan-list** permette di rimuovere una o più VLAN da un determinato trunk. Le quattro VLAN create sono state definite sul trunk. Rimuovere la VLAN 2 e la VLAN 3 con il comando [clear trunk 5/24 2-3](#) sulla VLAN e il comando [clear trunk 2/24 2-3](#) sulla VLAN Sb. Per controllare il risultato del comando **clear**, usare il comando [show trunk 5/24](#). Solo le VLAN 1 e 4 attraversano il trunk tra Sa e Sb. Il ping tra Sa e Sb ha esito negativo:

```
Sa> (enable) clear trunk 5/24 2-3
Removing Vlan(s) 2-3 from allowed list.
Port 5/24 allowed vlans modified to 1,4-1005.
Sa> (enable) show trunk 5/24
Port      Mode      Encapsulation  Status      Native vlan
-----
5/24     desirable dot1q           trunking    2

Port      Vlans allowed on trunk
-----
5/24     1,4-1005

Port      Vlans allowed and active in management domain
-----
5/24     1,4

Port      Vlans in spanning tree forwarding state and not pruned
-----
5/24     1,4
```

- Riattivare una VLAN. Per aggiungere nuovamente una VLAN su un trunk, usare il comando [set trunk module/port vlan-list](#).

```

Sa> (enable) set trunk 5/24 2
Adding vlans 2 to allowed list.
Port(s) 5/24 allowed vlans modified to 1-2,4-1005.
Sa> (enable) show trunk
Port          Mode          Encapsulation  Status          Native vlan
-----
5/24          desirable    dot1q           trunking        2

Port          Vlans allowed on trunk
-----
5/24          1-2,4-1005

Port          Vlans allowed and active in management domain
-----
5/24          1-2,4

Port          Vlans in spanning tree forwarding state and not pruned
-----
5/24          1-2,4

```

La VLAN 2 sta tornando a funzionare sul trunk. È possibile eseguire il ping tra Sa e Sb.

Errori comuni

VLAN native diverse

Si tratta di un errore di configurazione frequente. La VLAN nativa configurata su entrambe le estremità di un trunk 802.1Q deve essere la stessa. Tenere presente che uno switch che riceve un frame non contrassegnato lo assegna alla VLAN nativa del trunk. Se un'estremità è configurata per la VLAN nativa 1 e l'altra per la VLAN nativa 2, un frame inviato nella VLAN 1 da un lato viene ricevuto sulla VLAN 2 dall'altro. Il risultato è l'unione della VLAN 1 e della VLAN 2. Non c'è motivo di volerlo e ciò potrebbe comportare alcuni problemi di connettività nella rete.

Un dispositivo Cisco in genere avvisa l'utente della mancata corrispondenza della VLAN nativa. Vedere il passo 1 della sezione [Impostazione della VLAN nativa](#) per i tipi di messaggi di errore che si ricevono sulla console in questo caso. Verificare sempre che la VLAN nativa sia la stessa sulla configurazione trunk degli switch.

Domini VTP diversi

Quando si crea un trunk tra due switch e si utilizza la negoziazione DTP, verificare due volte che il dominio VTP configurato su entrambi gli switch sia lo stesso. La negoziazione non ha luogo tra due switch che si trovano in domini VTP diversi. L'esempio in questa sezione prende la configurazione di funzionamento del trunking descritta in precedenza.

Nota: anche se due switch si trovano in domini VTP diversi, è possibile comunicare tra loro se si aggiungono manualmente le VLAN su ciascuno switch. Sebbene vi sia una mancata corrispondenza del dominio VTP, la comunicazione VLAN funziona correttamente. Tuttavia, gli aggiornamenti VTP non vengono propagati tramite questo collegamento sulla VLAN in questione perché i domini sono diversi.

- Sa in modalità trunking desiderabile, incapsulamento dot1q
- Sb in modalità trunking automatica, negoziazione incapsulamento
- La stessa VLAN nativa e le stesse VLAN consentite su ciascun lato

L'unica differenza è che si assegna il dominio VTP "c" sulla SNA e il dominio VTP "cisco" sulla Sb:

Sa> (enable) **show trunk**

No ports trunking.

Sa> (enable) **show trunk 5/24**

Port	Mode	Encapsulation	Status	Native vlan
5/24	desirable	dot1q	not-trunking	1

Port Vlans allowed on trunk

5/24 1-1005

Port Vlans allowed and active in management domain

5/24 1

Port Vlans in spanning tree forwarding state and not pruned

5/24

Sb> (enable) **show trunk**

No ports trunking.

Sb> (enable) **show trunk 2/24**

Port	Mode	Encapsulation	Status	Native vlan
2/24	auto	negotiate	not-trunking	1

Port Vlans allowed on trunk

2/24 1-1005

Port Vlans allowed and active in management domain

2/24 1

Port Vlans in spanning tree forwarding state and not pruned

2/24

Sb> (enable)

Potete vedere che il bagagliaio non è salito. Se si verifica questo tipo di problema, controllare il dominio VTP configurato sugli switch. Usare il comando [show vtp domain](#):

Sa> (enable) **show vtp domain**

Domain Name	Domain Index	VTP Version	Local Mode	Password
c	1	2	server	-

Vlan-count Max-vlan-storage Config Revision Notifications

8 1023 0 disabled

Last Updater V2 Mode Pruning PruneEligible on Vlans

10.0.0.1 disabled disabled 2-1000

Sb> (enable) **show vtp domain**

Domain Name	Domain Index	VTP Version	Local Mode	Password
cisco	1	2	server	-

```

Vlan-count Max-vlan-storage Config Revision Notifications
-----
8          1023             20          disabled
-----
Last Updater V2 Mode Pruning PruneEligible on Vlans
-----
10.0.0.1     disabled disabled 2-1000

```

A questo punto, inserire lo switch sa nel dominio VTP "cisco" con il comando [set vtp domain cisco](#). Dopo alcuni secondi, il trunk viene negoziato e riattivato:

```

Sa> (enable) set vtp domain cisco
VTP domain cisco modified
Sa> (enable) 1997 May 13 13:59:22 %DTP-5-TRUNKPORTON:Port 5/24 has become dot1q trunk
1997 May 13 13:59:22 %PAGP-5-PORTFROMSTP:Port 5/24 left bridge port 5/24
1997 May 13 13:59:33 %PAGP-5-PORTTOSTP:Port 5/24 joined bridge port 5/24

```

Se si desidera mantenere domini VTP diversi ma creare comunque un trunk tra due switch, è necessario eseguire il trunking del codice hardware su ciascun lato del trunk (con l'uso di non negoziazione/attivato).

[Errore durante un tentativo di eliminare VLAN dell'intervallo esteso da una porta trunk](#)

Quando si tenta di eliminare le VLAN dell'intervallo esteso da una porta trunk con il comando [clear trunk](#), sulla console dello switch viene a volte visualizzato questo errore:

```

Failed to clear vlans in the extended range Maximum of 64 trunks can have
non-default extended range vlan configuration. Use the 'set trunk' command to restore
some existing entries to the default value.

```

Nota: il termine *intervallo esteso* include tutte le VLAN da 1025 a 4094. Il termine *intervallo esteso predefinito* include tutte le VLAN da 1025 a 4094. Se si tenta di cancellare una VLAN nell'intervallo da 1025 a 4094, la VLAN diventa l'*intervallo esteso non predefinito*. Il numero massimo di trunk che superano l'*intervallo esteso non predefinito* è 64. Sono inclusi sia i trunk inattivi che quelli attivi.

Questo errore e il limite di 64 trunk provengono dal blocco NVRAM che viene usato per archiviare configurazioni non predefinite per VLAN dell'intervallo esteso. Se si usa il comando [show trunk extended-range](#), è possibile visualizzare tutti i trunk configurati con intervalli estesi non predefiniti. Per impostazione predefinita, l'intera configurazione è archiviata nella NVRAM. La NVRAM ha diversi "blocchi" per salvare le configurazioni non predefinite. I blocchi vengono inseriti in diverse categorie, ad esempio globali o moduli. Il blocco che contiene la configurazione non predefinita per gli intervalli estesi ha un limite di 64 trunk.

Esistono due soluzioni per ridurre il numero di trunk estesi non di default. Il primo metodo consiste nel ripristinare le porte trunk non attive/inutilizzate sulle VLAN predefinite consentite. Usare il comando [set trunk mod/porta 1025-4094](#). Quindi, il comando [clear trunk mod/porta 1025-4094](#) dovrebbe funzionare sulle VLAN estese. La seconda soluzione è modificare la modalità di configurazione da binaria (predefinita) a testo. Per modificare la configurazione in modalità testo, usare il comando [set config mode text](#). La modalità testo utilizza in genere meno memoria NVRAM o Flash rispetto alla modalità di configurazione binaria.

Nota: quando si opera in modalità file di testo, la maggior parte delle impostazioni utente non

viene salvata immediatamente nella NVRAM; le modifiche alla configurazione vengono scritte solo nella memoria DRAM. Usare il comando [write memory](#) per archiviare la configurazione in un archivio non volatile. Per salvare automaticamente la configurazione del testo nella NVRAM, usare il comando **set config mode text auto-save**.

[Modalità trunking non compatibile con il tipo di incapsulamento](#)

Questo è un problema comune che ha iniziato a essere segnalato al [supporto tecnico Cisco](#) quando sono stati forniti i primi moduli che supportavano sia 802.1Q che ISL. Le persone sono state usate per la configurazione di un trunk con il comando **set trunk module/port on** o **set trunk module/port nonegotiate**. Il problema è che, per impostazione predefinita, il tipo di incapsulamento è impostato su NEGOTIate. Il tipo di incapsulamento NEGOTIate è supportato solo dalla modalità di trunking automatica o desiderata. I tipi di incapsulamento on e non negoziazione non eseguono alcuna negoziazione tra gli switch e devono essere impostati su ISL o 802.1Q quando sono configurati. Di seguito è riportato un registro di ciò che accade sullo switch in questo caso:

```
Sa> (enable) set trunk 5/24 on
Failed to set port 5/24 to trunk mode on.
Trunk mode 'on' not allowed with trunk encapsulation type 'negotiate'.
Sa> (enable) set trunk 5/24 nonegotiate
Failed to set port 5/24 to trunk mode nonegotiate.
Trunk mode 'nonegotiate' not allowed with trunk encapsulation type
'negotiate'.
Sa> (enable)
```

Ciò ha senso perché se non si negozia con il telecomando, come è possibile conoscere il tipo di incapsulamento (802.1Q o ISL) da utilizzare per richiamare il trunk? Esistono due possibilità:

- Utilizzare la modalità desiderata. In questo caso, negoziare la modalità di incapsulamento con il telecomando:

```
Sa> (enable) set trunk 5/24 desirable
Port(s) 5/24 trunk mode set to desirable.
Sa> (enable) 1997 May 09 17:49:19 %DTP-5-TRUNKPORTON:Port 5/24 has become
isl trunk
```

- Specificare l'incapsulamento da utilizzare:

```
Sa> (enable) set trunk 5/24 isl on
Port(s) 5/24 trunk mode set to on.
Port(s) 5/24 trunk type set to isl.
Sa> (enable) 1997 May 09 17:50:16 %DTP-5-TRUNKPORTON:Port 5/24 has become
isl trunk
```

[Comandi utilizzati nel documento](#)

[Riepilogo comandi](#)

- [ping](#)
- [set interface](#)
- [impostare il trunk](#)
- [set vlan](#)
- [set vtp domain](#)
- [show interface](#)
- [show port](#)
- [show port capabilities](#)

- [mostra trunk](#)
- [show vtp domain](#)

Informazioni correlate

- [Configurazione del trunking ISL sugli switch Catalyst serie 5500/5000 e 6500/6000](#)
- [Configurazione dei trunk VLAN sulle porte Fast Ethernet e Gigabit Ethernet](#)
- [Descrizione e configurazione del protocollo VLAN Trunk Protocol \(VTP\)](#)
- [Supporto dei prodotti LAN](#)
- [Supporto della tecnologia di switching LAN](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)