Trunking zwischen Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 unter Verwendung von 802.1Q-Kapselung mit Cisco CatOS-Systemsoftware

Inhalt

Einführung

In diesem Dokument wird das Konzept des Trunkings zwischen zwei Ethernet-Switches vorgestellt und der Schwerpunkt auf dem IEEE 802.1Q-Trunking-Standard gelegt. Nach einer kurzen Beschreibung des 802.1Q-Trunking-Mechanismus beschreibt das Dokument die Implementierung auf den Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000. Es wird ein vollständiges Beispiel sowie einige häufige Fehler in Bezug auf die 802.1Q-Trunking-Konfiguration unter Verwendung der Catalyst OS (CatOS)-Systemsoftware bereitgestellt. Beispiele für 802.1Q-Trunking mit Cisco IOS®-Systemsoftware finden Sie unter Konfigurieren von 802.1Q-Trunking zwischen Catalyst 3550/3560/3750- und Catalyst-Switches, die Cisco IOS-Software ausführen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

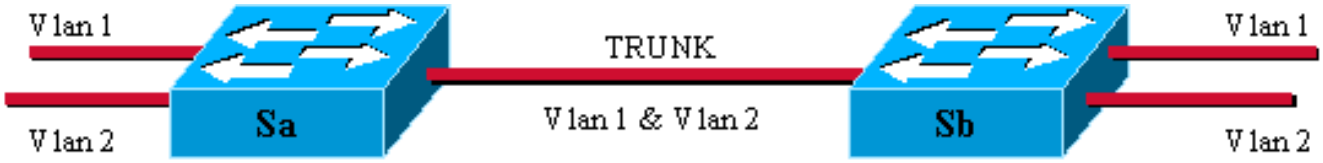
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Was ist ein Trunk?

In der Cisco Terminologie ist ein Trunk eine Point-to-Point-Verbindung, die mehrere VLANs überträgt. Der Zweck eines Trunks besteht darin, Ports zu speichern, wenn eine Verbindung zwischen zwei Geräten erstellt wird, die VLANs implementieren, in der Regel zwei Switches. In diesem Diagramm sind zwei VLANs enthalten, die auf zwei Switches verfügbar sein sollen: Sa und Sb. Die erste einfache Methode zur Implementierung besteht darin, zwei physische Verbindungen zwischen den Geräten zu erstellen. Die physischen Verbindungen übertragen den Datenverkehr für ein VLAN:

Natürlich ist diese Lösung nicht skalierbar. Wenn Sie ein drittes VLAN hinzufügen möchten, müssen Sie zwei zusätzliche Ports opfern. Dieses Design ist auch hinsichtlich der Lastverteilung ineffizient. Der Datenverkehr in einigen VLANs rechtfertigt unter Umständen keine dedizierte Verbindung. Ein Trunk bündelt virtuelle Verbindungen über eine physische Verbindung, wie in diesem Diagramm gezeigt:



Hier kann der Datenverkehr für jedes VLAN über die eindeutige physische Verbindung zwischen den beiden Switches übertragen werden. Um dies zu erreichen, wird jeder auf der Verbindung gesendete Frame von Sa markiert, sodass Sb das VLAN kennt, zu dem er gehört. Es gibt verschiedene Tagging-Schemata. Die häufigsten Ethernet-Segmente sind:

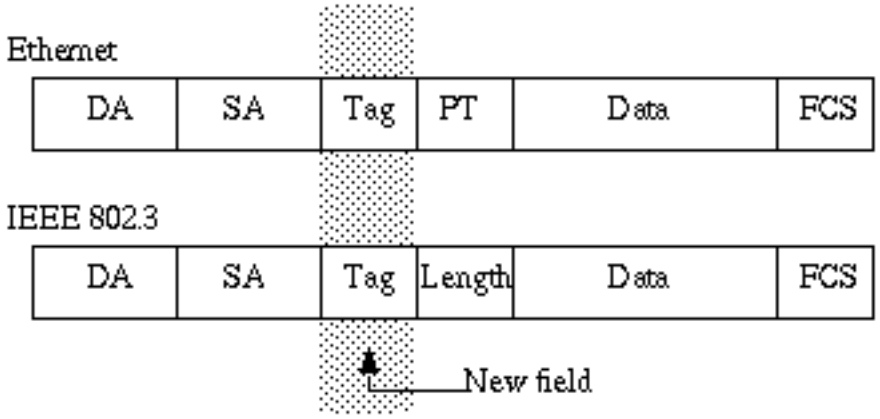
- Inter-Switch Link (ISL) (das ursprüngliche proprietäre ISL-Protokoll von Cisco)
- 802.1Q (der IEEE-Standard, auf den sich dieses Dokument konzentriert)

Grundlegende Merkmale von 802.1Q-Trunking

Tagging-Mechanismus

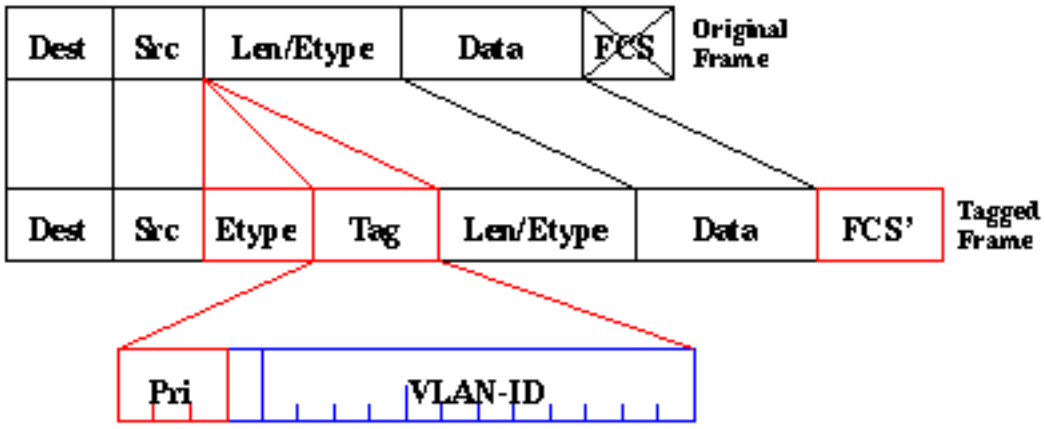
802.1Q verwendet einen internen Tagging-Mechanismus. Intern bedeutet, dass ein Tag im Frame eingefügt wird:

Hinweis: Bei ISL wird der Frame gekapselt.



Hinweis: Auf einem 802.1Q-Trunk ist ein VLAN NICHT markiert. Dieses VLAN mit dem Namen des nativen VLAN muss auf jeder Seite des Trunks gleich konfiguriert werden. Auf diese Weise können Sie bestimmen, zu welchem VLAN ein Frame gehört, wenn Sie einen Frame ohne Tag erhalten.

Der Tagging-Mechanismus impliziert eine Änderung des Frames. Das Trunking-Gerät fügt ein 4-Byte-Tag ein und berechnet die Frame Check Sequence (FCS) neu:



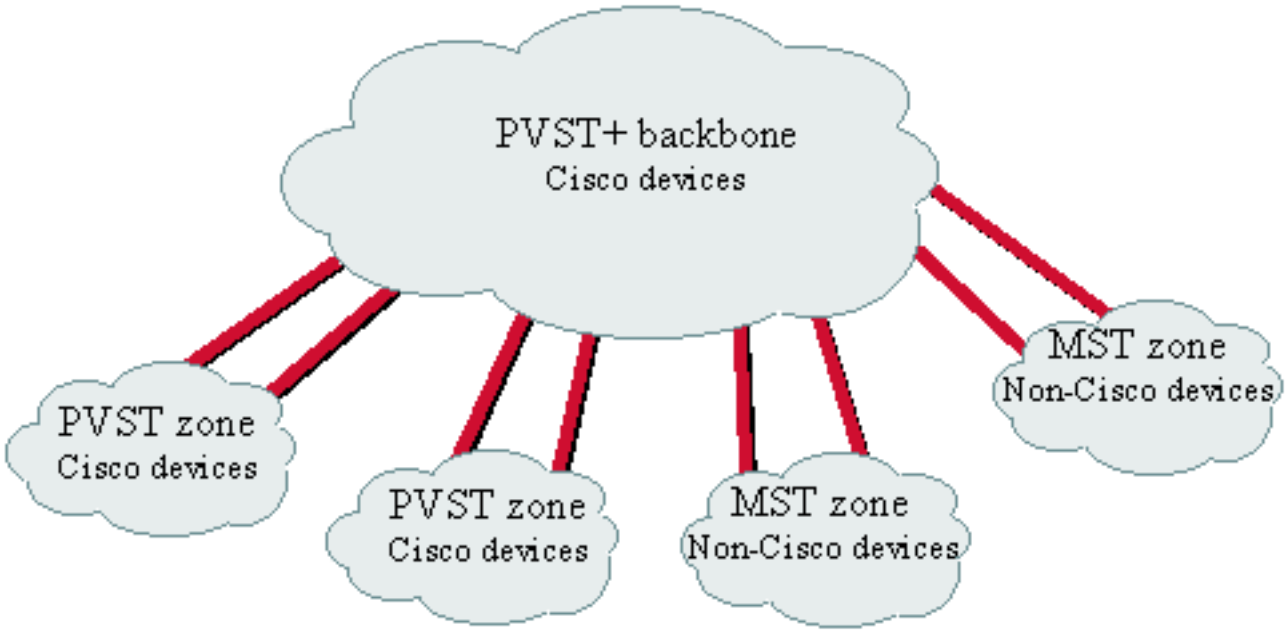
Das EtherType-Feld, das den 802.1Q-Frame identifiziert, ist 0x8100. Zusätzlich zur 12-Bit-VLAN-ID sind 3 Bit für IEEE 802.1p-Prioritäts-Tagging reserviert.

Hinweis: Durch das Einfügen eines Tags in einen Frame, der bereits die maximale Ethernet-Größe aufweist, wird ein 1522-Byte-Frame erstellt, der vom Empfangsgerät als "Babygigant" angesehen werden kann. Der IEEE 802.3-Ausschuss erweitert die maximale Standard-Frame-

Größe, um dieses Problem anzugehen.

Überlegungen zum Spanning Tree

Der 802.1Q-Standard ist mehr als nur ein Tagging-Mechanismus. Außerdem wird eine eindeutige Spanning Tree-Instanz definiert, die im nativen VLAN für alle VLANs im Netzwerk ausgeführt wird. Ein solches Mono Spanning Tree (MST)-Netzwerk bietet im Vergleich zu einem PVST-Netzwerk (Per VLAN Spanning Tree), das pro VLAN eine Instanz des Spanning Tree Protocol (STP) ausführt, keine gewisse Flexibilität. Cisco hat PVST+ entwickelt, um die Ausführung mehrerer STP-Instanzen (auch über ein 802.1Q-Netzwerk) mithilfe eines Tunneling-Mechanismus zu ermöglichen. Obwohl dieses Dokument über den Umfang dieses Dokuments hinausgeht, kann es kurz als Verwendung eines Cisco Geräts beschrieben werden, um eine MST-Zone (in der Regel das 802.1Q-basierte Netzwerk eines anderen Anbieters) mit einer PVST-Zone (in der Regel ein Cisco ISL-basiertes Netzwerk) zu verbinden. Es ist keine spezielle Konfiguration zum Erreichen dieses Ziels einzugeben. Im Idealfall sollte eine gemischte Umgebung wie dieses Diagramm aussehen:



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

Cisco Implementierung

In der aktuellen Implementierung unterstützen Cisco Geräte nur VLAN-Nummern bis 1005. Diese Einschränkung, die eingeführt wurde, um der Anzahl der mit ISL verfügbaren VLANs zu entsprechen, ist nach dem 802.1Q-Standard zulässig. Cisco hat in CatOS 5.1 eine VLAN-Zuordnungsfunktion implementiert, um die Interoperabilität mit Geräten anderer Hersteller zu vereinfachen. Diese Funktion ist jedoch selten erforderlich.

Hinweis: Informationen zur VLAN-Zuordnungsfunktion finden Sie unter Konfigurieren von VLANs.

Cisco hat außerdem sein Dynamic ISL (DISL)-Protokoll angepasst und in Dynamic Trunking Protocol (DTP) umgewandelt. DISL kann ISL-Trunking für eine Verbindung zwischen zwei

Geräten aushandeln. DTP kann darüber hinaus die Trunking-Kapselung (802.1Q oder ISL) aushandeln, die ebenfalls verwendet wird. Dies ist eine interessante Funktion, da einige Cisco Geräte nur ISL oder 802.1Q unterstützen, während einige beide Geräte verwenden können.

Bei der Implementierung von Cisco ist ein Trunk eine Point-to-Point-Verbindung. Es ist jedoch möglich, die 802.1Q-Kapselung für ein Ethernet-Segment zu verwenden, das von mehr als zwei Geräten gemeinsam genutzt wird. Eine solche Konfiguration ist selten erforderlich, ist aber bei der Deaktivierung der DTP-Aushandlung noch möglich.

802.1Q-Trunks konfigurieren

Hardware-/Softwareanforderungen

Aus Software-Sicht war die 802.1Q-Kapselung erstmals mit CatOS Software 4.1 sichtbar. In dieser Version musste die Trunking-Konfiguration hartkodiert werden. DTP wurde nur mit CatOS 4.2 angezeigt. Weitere Informationen finden Sie im Abschnitt DTP-Modi dieses Dokuments.

Nicht alle Catalyst-Ports unterstützen die 802.1Q-Kapselung. Während derzeit Catalyst 4500/4000-Switches nur 802.1Q unterstützen, können die Ports der Catalyst 6500/6000-Serie 802.1Q- oder ISL-Kapselung verwenden. Je nach Modul können Catalyst 5500/5000-Trunk-fähige Ports 802.1Q-Kapselung, ISL-Kapselung oder beides verwenden. Die beste Möglichkeit, dies auszuchecken, ist die Verwendung des Befehls **show port functions**. Die Trunking-Kapazität ist explizit angegeben:

```
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
```

DTP-Modi

Wenn Sie einen Port für das Trunking konfigurieren, können Sie zwei Parameter festlegen: den Trunking-Modus und den Kapselungstyp (wenn DTP auf diesem Port unterstützt wird).

- Der **Trunking-Modus** definiert, wie der Port die Einrichtung eines Trunks mit seinem Peer-Port aushandelt. Hier finden Sie eine Liste der möglichen Einstellungen:Achten Sie darauf, dass einige Modi (*on*, *nonegotiate*, *off*) explizit angeben, in welchem Zustand der Port endet. Eine fehlerhafte Konfiguration kann zu einem gefährlichen, inkonsistenten Zustand führen, in dem eine Seite Trunking (Trunking), die andere Seite nicht.Ein Port *auf*, *automatisch* oder *wünschenswert* sendet regelmäßig DTP-Frames. Ein Trunking-Port in *Auto* oder *wünschenswert* geht zurück zum Non-Trunking, wenn er innerhalb von 5 Minuten keine DTP-Aktualisierung von seinem Nachbarn erhält.**Hinweis:** Wenn Sie die CatOS-Software 4.1

ausführen, müssen Sie jede Form der Aushandlung deaktivieren, indem Sie den ***Aus-*** oder ***Unegotiate-Modus*** verwenden, wenn Sie 802.1Q-Trunking konfigurieren.
- Mit dem **Kapselungstyp** kann der Benutzer angeben, ob beim Einrichten des Trunks 802.1Q oder ISL verwendet werden soll. Natürlich ist der Parameter nur relevant, wenn das Modul, das Sie verwenden, beide verwenden kann. Der Parameter kann drei verschiedene Werte haben:

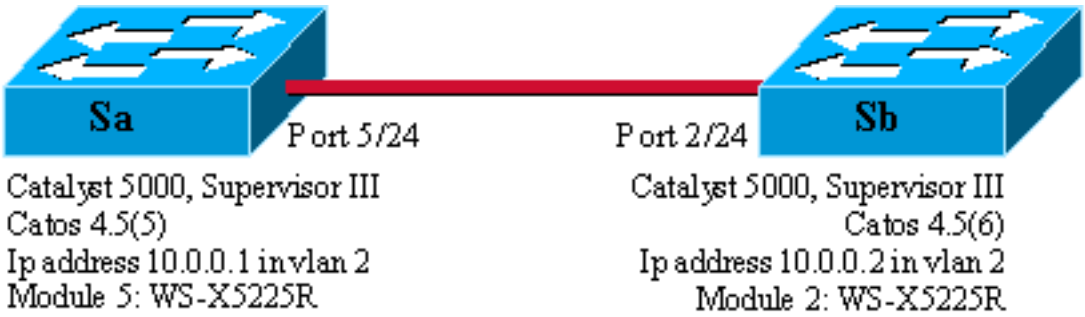
Im Abschnitt *"Ergebnisse der möglichen Fast Ethernet- und Gigabit Ethernet-Trunk-Konfigurationen"* unter Konfigurieren von VLAN-Trunks auf Fast Ethernet- und Gigabit Ethernet-Ports finden Sie eine Liste aller möglichen Konfigurationen.

Hinweis: Zwischen zwei Switches in unterschiedlichen VLAN Trunk Protocol (VTP)-Domänen wird keine Aushandlung durchgeführt. Weitere Informationen finden Sie unter Konfigurieren von VTP.

Schritt-für-Schritt-Beispiel

Netzwerkdiagramm

Dieses Beispiel basiert auf einer sehr einfachen Laboreinrichtung, die zwei Catalyst 5500/5000-Switches umfasst, die über Trunk-fähige Ports miteinander verbunden sind. Sie benötigen ein Crossover-Kabel, um zwei Switches miteinander zu verbinden.



Minimale Einrichtung eines 802.1Q-Trunks mit Verbindungstests

Gehen Sie wie folgt vor:

1. Überprüfen Sie, ob die Status der Ports aktiv, aber nicht Trunking sind.Schließen Sie ein Terminal an die Konsole Ihrer Switches an. Weitere Informationen finden Sie im Dokument Verbinden eines Terminals mit dem Konsolenport von Catalyst-Switches (falls erforderlich). Überprüfen Sie zunächst den Status des Ports, der an der Einrichtung beteiligt ist. Verwenden Sie den Befehl **Port 5/24** auf Sa anzeigen (**Port 2/24** auf Sb anzeigen) und überprüfen Sie, ob der Status verbunden ist:

```
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.
```

Sie haben den Standardwert für diesen Port. Es wurde bei der Aushandlung von 100-MB-Vollduplex verwendet und ist VLAN 1 zugewiesen. Geben Sie den Befehl **show trunk 5/24** ein, um deutlich zu machen, dass der Port kein Trunking ist und über einen automatischen

Standardmodus und eine Aushandlung der Kapselung verfügt.

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

2. Legen Sie eine IP-Adresse für die sc0-Verwaltungsschnittstellen fest.Verwenden Sie den Befehl set interface sc0 10.0.0.1 auf Switch Sa und den Befehl **set interface sc0 10.0.0.2** auf Switch Sb, um den beiden Switches eine IP-Adresse zuzuweisen. Der Befehl **show interface** bestätigt, dass die Verwaltungsschnittstelle jetzt korrekt im Standard-VLAN 1 eingestellt ist:

```
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)
```

   Wenn Sie den Befehl **show interface** von Ihrem Cisco Gerät ausgeben, können Sie Output Interpreter (nur registrierte Kunden) verwenden, um potenzielle Probleme und Fixes anzuzeigen.

3. Überprüfen Sie die Verbindung zwischen SA und Sb.Führen Sie den Befehl **ping 10.0.0.2** von Switch Sa aus, um zu beweisen, dass Switch Sb jetzt erreicht werden kann:

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

4. Konfigurieren Sie dieselbe VTP-Domäne auf beiden Switches.Weisen Sie nun beiden Switches die gleiche VTP-Domäne zu. Wie Sie gesehen haben, ist die Verwendung derselben VTP-Domäne für die Verwendung der DTP-Aushandlung obligatorisch. Geben Sie den Befehl set vtp domain cisco auf beiden Switches ein, um sie mit dem Domänennamen "cisco" zu konfigurieren:

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

5. Erstellen Sie in jedem Switch ein VLAN 2.Geben Sie den Befehl **set vlan 2** auf beiden Switches ein, um das VLAN 2 zu erstellen. Wenn die Switches bereits über einen Trunk verbunden waren, müssten Sie den Befehl nur auf einem Switch ausführen, während der andere Switch ihn automatisch über VTP erfährt. Da Sie noch keinen Trunk haben, gibt es keine VTP-Kommunikation zwischen SA und Sb:

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

6. Ändern Sie die Verwaltungsschnittstellen in VLAN 2.Sie verschieben nun die Verwaltungsschnittstelle beider Switches in VLAN 2. Auf diese Weise zeigen Sie, dass es keine Kommunikation zwischen Sa und Sb gibt, bevor ein Trunk hergestellt wird. Geben Sie den Befehl **set interface sc0 2** auf jedem Switch ein, um die sc0-Schnittstelle in VLAN 2 zu verschieben. Geben Sie den Befehl **show interface** ein, um zu überprüfen, ob der Befehl wirksam ist:

```
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. Überprüfen Sie, ob die Verbindung zwischen den beiden Switches getrennt ist.Jetzt schlägt der **Ping 10.0.0.2** an Sb von Sa ab, was beweist, dass in VLAN 2 keine Verbindung zwischen den Switches besteht:

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

8. Überprüfen Sie die Portfunktionen.Bevor Sie mit der Konfiguration eines Trunks beginnen, können Sie mit dem Befehl **show port functions** überprüfen, dass beide Ports 802.1Q-Trunking implementieren können:

```
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. Konfigurieren Sie die Trunk-Kapselung auf 802.1Q.Nun muss der Trunk auf Sa konfiguriert werden. In Schritt 1 haben Sie gesehen, dass sich beide Ports im standardmäßigen Trunking-Modus Auto (Automatisch) befanden und der Kapselungstyp aushandeln. Eine Kombination aus Auto und Auto führt keinen Trunk aus. Dies ist normal. Jede Seite ist bereit, Trunk zu werden, wird dies jedoch nur tun, wenn die Remote-Seite dies anfordert. Unter Berücksichtigung der Standardkonfiguration:Sie müssen nur den Trunk-Modus auf einer Seite in "wünschenswert" ändern, um den Trunk zu aktivieren. Der Grund hierfür ist, dass ein Port im wünschenswerten Modus seinem Nachbarn mitteilt, dass er Trunking nutzen möchte. Da die Fernbedienung (im automatischen Modus) bei entsprechender Aufforderung zum Trunking wechselt, reicht dies aus, um den Trunk zu aktivieren.Wenn Sie die Kapselung dot1q auf einer Subschnittstelle konfigurieren, bedeutet dies, dass das VLAN seit der internen Verwendung im System nicht mehr verwendet werden kann. Der 6500 oder 7600 weisen das VLAN zu und machen diese Subschnittstelle dann zum einzigen Mitglied. Es ist also nicht möglich, ein VLAN zu haben und dann zu versuchen, es in einer Subschnittstelle oder umgekehrt zu verwenden. Um dieses Problem zu beheben, erstellen Sie statt Subschnittstellen Trunk-Ports, sodass das VLAN auf allen Schnittstellen sichtbar ist. Wenn Subschnittstellen erforderlich sind, können die in den Subschnittstellen hinzugefügten VLANs an anderen Ports nicht verwendet werden.Sie müssen auch angeben, welche Kapselung Sie verwenden möchten. Dies liegt daran, dass beide Ports ISL-fähig sind. Diese Kapselung wird zuerst ausgewählt, wenn beide Enden im Aushandlung-Modus sind.Die Syntax des Befehls lautet: **Trunk-*Modul/Port* einstellen [ein | Aus | Wünschenswert | Auto | nonegotiate] [vlan_range] [isl] | dot1q | verhandeln]**. Geben Sie den Befehl **set trunk 5/24 dot1q wünschenswert** auf Switch-SA aus:

```
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. Überprüfen Sie, ob der Trunk aktiv ist.Das Konsolenprotokoll des vorherigen Befehls zeigt eindeutig, dass der Port zu Trunking verschoben wurde. Sie können jedoch auch den Befehl **show trunk 5/24** auf Sa und den Befehl show trunk 2/24 auf Sb ausführen, um zu überprüfen. Sie sehen einen kleinen Unterschied zwischen den beiden Ausgängen:Der Port auf Sa befindet sich im wünschenswerten Modus, während sich der Sb-Port im Auto-Modus befindet.Interessanter ist, dass die Kapselung dot1q auf Sa ist, während es **n-dot1q** auf Sb. Dies soll zeigen, dass Sb seine Kapselung auf dot1q ausgehandelt hat. Wenn Sie keine Kapselung für Sa angegeben haben, wären beide Ports in der n-isl-Kapselung angekommen:

```
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.
```

Wenn Sie die Ausgabe eines Befehls **show trunk** von Ihrem Cisco Gerät haben, können Sie Output Interpreter (nur registrierte Kunden) verwenden, um potenzielle Probleme und Fixes anzuzeigen.

11. Überprüfen Sie die Konnektivität.Sie können überprüfen, ob VLAN 2 nun Ihren Trunk durchläuft, indem Sie einfach Sb von Sa: pingen.

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

Festlegen des nativen VLANs

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl **set vlan ein**.Der Befehl "set vlan 2 5/24" dient dazu, einem bestimmten VLAN einen Port zuzuweisen. Bei einem Trunking-Port wird das native VLAN in VLAN 2 geändert. Natürlich müssen Sie das Gleiche auf SB mit set VLAN 2 2/24 tun:

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

```
Sa> (enable)
```

Bevor Sie das native VLAN auf Sb ändern, besteht nun eine Inkonsistenz zwischen der Sa- und der Sb-Konfiguration. Die beiden Enden des Trunks verfügen nicht über dieselbe native VLAN-Konfiguration. Hier werden einige Warnmeldungen auf der USB-Konsole angezeigt.**Hinweis:** Der Switch, der Inkonsistenzen meldet, kann variieren, je nachdem, welche der beiden Switches die Root Bridge für die VLANs 1 und 2 ist.

```
Sb> (enable) 2000 Dec 07 16:31:24 %SPANTREE-2-RX_1QPVIDERR: Rcved
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.
```

Die systemeigene VLAN-Diskrepanz wurde behoben, und alles geht zurück zum normalen Modus.

2. Überprüfen Sie das Ergebnis.Überprüfen Sie jetzt einfach das Ergebnis dieser Befehle auf Ihrem Trunk mit dem Befehl **show trunk 5/24**:

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

<
```

Geben Sie die für den Trunk zulässigen VLANs an.

Gehen Sie wie folgt vor:

1. Erstellen Sie zusätzliche VLANs.Wenn Sie einen neuen Trunk erstellen, werden standardmäßig alle vorhandenen VLANs im Netzwerk übergeben. Sie erfahren, wie Sie die Liste der zulässigen VLANs für einen Trunk einschränken. Zunächst müssen Sie zwei zusätzliche VLANs erstellen (3 und 4). Beispielsweise können Sie den Befehl set vlan 3 und den Befehl **set vlan 4** auf Sa ausführen, um die zusätzlichen VLANs zu erstellen. Sie müssen den Befehl nur auf einem Switch eingeben. VTP leitet diese Informationen an den anderen Switch weiter.**Hinweis:** Dieser Teil der Konfiguration ist unabhängig davon, ob eine 802.1Q- oder ISL-Kapselung verwendet wird, identisch.

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

2. Entfernen Sie VLANs aus dem Trunk.Mit dem Befehl **clear trunk *module/port vlan-list* können Sie ein oder mehrere VLANs aus einem bestimmten Trunk entfernen.** Hier wurden die vier von Ihnen erstellten VLANs auf Ihrem Trunk definiert. Entfernen Sie VLAN 2 und VLAN 3 mit dem Befehl **clear trunk 5/24 2-3** auf Sa und dem Befehl **clear trunk 2/24 2-3** auf Sb. Sie

können das Ergebnis des **clear**-Befehls mithilfe des Befehls show trunk 5/24 überprüfen. Nur die VLANs 1 und 4 überqueren nun den Trunk zwischen Sa und Sb. Ein Ping zwischen SA und Sb schlägt jetzt fehl:

```
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
```

3. Aktivieren Sie ein VLAN.Um ein VLAN wieder zu einem Trunk hinzuzufügen, verwenden Sie den Befehl **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
```

VLAN 2 fließt nun wieder im Trunk. Ein Ping von SA an Sb ist möglich.

Häufige Fehler

Verschiedene native VLANs

Dies ist ein häufiger Konfigurationsfehler. Das native VLAN, das auf jedem Ende eines 802.1Q-Trunks konfiguriert wird, muss identisch sein. Denken Sie daran, dass ein Switch, der einen Frame ohne Tags empfängt, diesen dem nativen VLAN des Trunks zuweist. Wenn ein Ende für natives VLAN 1 und das andere für natives VLAN 2 konfiguriert ist, wird ein Frame, der in VLAN 1 auf der einen Seite gesendet wird, auf der anderen Seite in VLAN 2 empfangen. Dies führt zum Zusammenführen von VLAN 1 und 2. Es gibt keinen Grund, warum Sie das wünschen, und es kann einige Verbindungsprobleme in Ihrem Netzwerk implizieren.

Ein Cisco Gerät warnt Sie in der Regel vor einem nativen VLAN-Konflikt. In Schritt 1 des Abschnitts Festlegen des nativen VLANs finden Sie die Fehlermeldungen, die Sie in diesem Fall auf der Konsole erhalten. Überprüfen Sie immer, ob das native VLAN für die Trunk-Konfiguration Ihrer Switches identisch ist.

Unterschiedliche VTP-Domänen

Wenn Sie einen Trunk zwischen zwei Switches erstellen und DTP-Aushandlung verwenden, überprüfen Sie, ob die auf beiden Switches konfigurierte VTP-Domäne identisch ist. Zwischen zwei Switches in unterschiedlichen VTP-Domänen findet keine Aushandlung statt. Im Beispiel in diesem Abschnitt wird die oben beschriebene funktionierende Trunking-Konfiguration beschrieben.

Hinweis: Auch wenn sich zwei Switches in unterschiedlichen VTP-Domänen befinden, können Sie die Kommunikation zwischen diesen Switches ermöglichen, wenn Sie auf jedem Switch VLANs manuell hinzufügen. Obwohl eine VTP-Domäne nicht übereinstimmt, funktioniert die VLAN-Kommunikation einwandfrei. VTP-Updates werden jedoch nicht über diesen Link in diesem VLAN weitergeleitet, da sich die Domänen unterscheiden.

- Sa im Trunking-Modus wünschenswert, encapsulation dot1q
- Sb im Trunking-Modus automatisch, Kapselung aushandeln
- dasselbe native VLAN und dieselben VLANs, die auf beiden Seiten zulässig sind

Der einzige Unterschied besteht darin, dass Sie der VTP-Domäne "c" auf SA und der VTP-Domäne "**cisco**" auf 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)
```

Sie können sehen, dass der Trunk nicht angezeigt wurde. Wenn dieses Problem auftritt, überprüfen Sie die auf den Switches konfigurierte VTP-Domäne. Geben Sie den Befehl **show vtp domain** ein:

```
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
```

Legen Sie Switch Sa jetzt mithilfe des Befehls **set vtp domain cisco** in die VTP-Domäne "cisco" ein. Nach einigen Sekunden wird der Trunk ausgehandelt und wieder aktiviert:

```
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
```

Wenn Sie verschiedene VTP-Domänen beibehalten, aber dennoch einen Trunk zwischen zwei Switches erstellen möchten, müssen Sie Code-Trunking auf jeder Seite des Trunks (mit nicht ausgehender/aktiver Verwendung) fest programmieren.

Fehler beim Versuch, VLANs mit großem Bereich von einem Trunk-Port zu löschen

Wenn Sie versuchen, die VLANs mit erweitertem Bereich von einem Trunk-Port mithilfe des Befehls **clear trunk** zu löschen, wird dieser Fehler manchmal in der Switch-Konsole angezeigt:

```
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.
```

Hinweis: Der Begriff *erweiterter Bereich* schließt jedes VLAN zwischen 1025 und 4094 ein. Der Begriff *erweiterter Standardbereich* umfasst alle VLANs von 1025 bis 4094. Wenn Sie versuchen, ein VLAN im Bereich von 1025 bis 4094 zu löschen, wird das VLAN zum *nicht standardmäßigen erweiterten Bereich*. Die maximale Anzahl von Trunks, die den *nicht standardmäßigen erweiterten Bereich* passieren, beträgt 64. Dies umfasst inaktive und aktive Trunks.

Dieser Fehler und die Beschränkung auf 64 Trunks stammen aus dem NVRAM-Block, der zum Speichern von nicht standardmäßigen Konfigurationen für VLANs mit erweitertem Bereich verwendet wird. Wenn Sie den Befehl **show trunk extended-range** (erweiterter Bereich anzeigen) ausführen, werden alle Trunks angezeigt, die mit nicht standardmäßigen erweiterten Bereichen konfiguriert sind. Standardmäßig wird die gesamte Konfiguration im NVRAM gespeichert. Der NVRAM verfügt über verschiedene "Blöcke" zum Speichern der nicht standardmäßigen Konfigurationen. Die Blöcke werden in verschiedene Kategorien eingeteilt, z. B. global oder module. Der Block mit der Nicht-Standardkonfiguration für erweiterte Bereiche ist auf 64 Trunks beschränkt.

Es gibt zwei Workarounds, um die Anzahl der nicht standardmäßigen erweiterten Trunks zu reduzieren. Die erste Methode besteht darin, alle nicht aktiven/nicht verwendeten Trunk-Ports auf die standardmäßig zulässigen VLANs zurückzusetzen. Verwenden Sie den Befehl **set trunk *mod/port* 1025-4094**. Der Befehl **clear trunk *mod/port* 1025-4094** sollte für die erweiterten VLANs funktionieren. Die zweite Lösung besteht darin, den Konfigurationsmodus von binär (Standard) in textbezogen zu ändern. Verwenden Sie den Befehl **set config mode text**, um den Konfigurationsmodus in den Textmodus zu ändern. Der Textmodus belegt in der Regel weniger NVRAM- oder Flash-Speicher als der Binärkonfigurationsmodus.

Hinweis: Beim Betrieb im Textdateikonfigurationsmodus werden die meisten Benutzereinstellungen nicht sofort im NVRAM gespeichert. Konfigurationsänderungen werden nur in DRAM geschrieben. Sie müssen den Befehl **write memory** ausführen, um die Konfiguration im nichtflüchtigen Speicher zu speichern. Verwenden Sie den Befehl **set config mode text auto-save**, um die Textkonfiguration im NVRAM automatisch zu speichern.

Der Trunking-Modus ist nicht mit dem Kapselungstyp kompatibel.

Dies ist ein häufiges Problem, das beim technischen Support von Cisco zur Sprache kam, als die ersten Module, die sowohl 802.1Q als auch ISL unterstützen konnten, ausgeliefert wurden. Die Konfiguration eines Trunks wurde mithilfe des Befehls **set trunk *module/port* on** oder **set trunk module/port nonegotiate** verwendet. Das Problem besteht darin, dass der Kapselungstyp standardmäßig auf "Negotiation" eingestellt ist. Der Aushandeln-Kapselungstyp wird nur von den automatischen oder wünschenswerten Trunking-Modi unterstützt. Die Ein- und Nicht-Eotiate-Kapselungstypen führen keine Verhandlungen zwischen Switches aus und müssen bei der Konfiguration auf ISL- oder 802.1Q-Kapselung fest eingestellt sein. Hier sehen Sie ein Protokoll der Ereignisse auf dem Switch in diesem Fall:

```
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)
```

Das ist sinnvoll, denn wenn Sie nicht mit der Fernbedienung verhandeln, wie würden Sie wissen, welche Art von Kapselung (802.1Q oder ISL) Sie verwenden sollten, um den Trunk zu aktivieren? Es gibt zwei Möglichkeiten:

- Verwenden Sie den erwünschten Modus. In diesem Fall handeln Sie den Kapselungsmodus mit dem Remote aus:

```
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
```

- Geben Sie die zu verwendende Kapselung an:

```
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
```

Im Dokument verwendete Befehle

Befehlsübersicht

- Ping
- Set-Schnittstelle
- Set-Trunk
- Set-VLAN
- VTP-Domäne festlegen
- Anzeigeschnittstelle
- Anzeigeport
- Portfunktionen anzeigen
- Hauptleitung
- VTP-Domäne anzeigen

Zugehörige Informationen

- Konfigurieren von ISL-Trunking auf Catalyst Switches der Serien 5500/5000 und 6500/6000
- Konfigurieren von VLAN-Trunks auf Fast Ethernet- und Gigabit Ethernet-Ports
- VTP (VLAN Trunk Protocol)
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems