

Konfigurationsbeispiel für Catalyst Express Switches der Serie 500

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Erstkonfiguration des Switches](#)

[Smartports](#)

[Smartport-Rollen](#)

[Smartport-Rollen auf Ports anwenden](#)

[Einschränkungen](#)

[Anwenden einer Smartports-Rolle auf einen einzelnen Port](#)

[Anwenden einer Smartports-Rolle auf alle Ports](#)

[Erstellen/Löschen von VLANs](#)

[VLAN-Typen](#)

[VLAN-Mitgliedschaft ändern](#)

[Konfigurieren von EtherChannels](#)

[Konfigurieren von Inter-VLAN-Routing mit einem Cisco Router](#)

[SPAN \(Switched Port Analyzer\) konfigurieren](#)

[Setzen Sie den Catalyst Express 500-Switch auf die werkseitigen Standardeinstellungen zurück.](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird das Verfahren beschrieben, mit dem Sie Switches der Cisco Catalyst Express 500-Serie für Smartport-Rollen, VLANs, EtherChannels, Switch Port Analyzer (SPAN) konfigurieren und VLAN-weites Routing mit Switches der Cisco Catalyst Express 500-Serie durchführen.

[Voraussetzungen](#)

[Anforderungen](#)

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- EtherChannels
- Inter-VLAN-Routing
- SPAN

Konfigurieren Sie den Cisco Catalyst Switch der Serie 500 mit den ursprünglichen Netzwerkeinstellungen, wie im Abschnitt [Erstkonfiguration](#) dieses Dokuments beschrieben.

Im Datenblatt für die Cisco Catalyst Switches der Serie 500 finden Sie Informationen zu den verschiedenen Modellen und den unterstützten Funktionen der [Cisco Catalyst Express Switches der Serie 500](#).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst Express 500G-12TC mit Cisco IOS® Software Release 12.2(25)FY
- Cisco 2800 Router, der IEEE 802.1Q-Trunk-Kapselung unterstützt.
- Cisco Catalyst Switches der Serie 3750 unterstützen die 802.1Q-Trunk-Kapselung.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

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

Erstkonfiguration des Switches

Führen Sie diese Schritte aus, um die Ersteinrichtung des Switches durchzuführen. Weitere Informationen zum Konfigurationsverfahren finden Sie im [Einführungsleitfaden für Catalyst Express 500 Switches](#).

1. Stellen Sie sicher, dass keine Verbindung zum Switch besteht.
2. Schalten Sie den Switch ein.
3. Warten Sie, bis die SETUP LED-Anzeige grün blinkt.
4. Klicken Sie auf **Setup**. Eine Switch-Port-LED fängt an, grün zu blinken.
5. Wenn eine Switch-Port-LED grün blinkt, schließen Sie Ihren PC an diesen Port an. Der LAN-Adapter dieses PCs muss so konfiguriert sein, dass er die IP-Adresse über DHCP abrufen kann. Die LEDs am PC und der Switch-Port blinken grün, während der Switch die Verbindung konfiguriert (dies dauert etwa eine Minute).
6. Öffnen Sie einen Webbrowser. Gehen Sie wie folgt vor, wenn der Browser die Benutzeroberfläche nicht automatisch aufruft: Geben Sie den Befehl **ipconfig** aus, um die dynamische Adresszuweisung anzuzeigen.

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

Windows 2000 IP Configuration

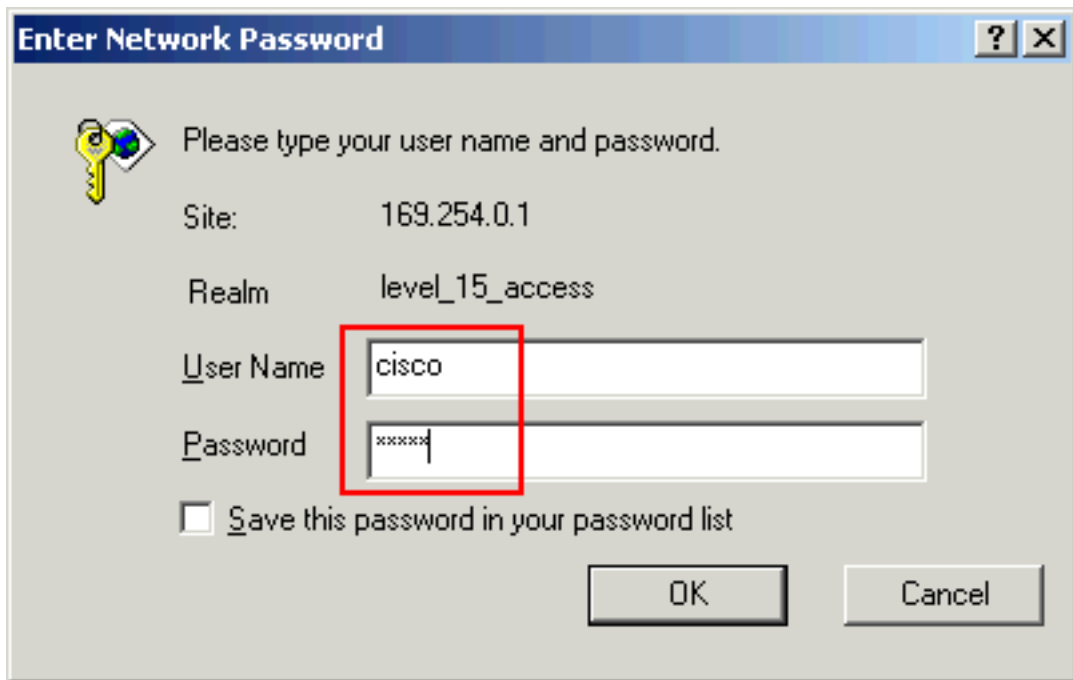
Ethernet adapter Local Area Connection:

    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
```

Der Switch konfiguriert seine Management-Adresse als Standard-Gateway für die LAN-Adapterkarte des PCs. **Hinweis:** Bei Versionen der Cisco IOS Software der Serie **FY** lautet die Management-IP-Adresse 10.0.0.1. Bei **SEG**-Versionen der Cisco IOS Software lautet die IP-Adresse 169.254.0.1. Gehen Sie vom Browser zur angegebenen IP-Adresse. Beispiel: <http://169.254.0.1>.

- 7. Geben Sie die Netzwerkeinstellungen und (falls erforderlich) die optionalen Einstellungen ein. Klicken Sie auf **Senden**, um die Änderungen zu speichern und die Basiskonfiguration abzuschließen.

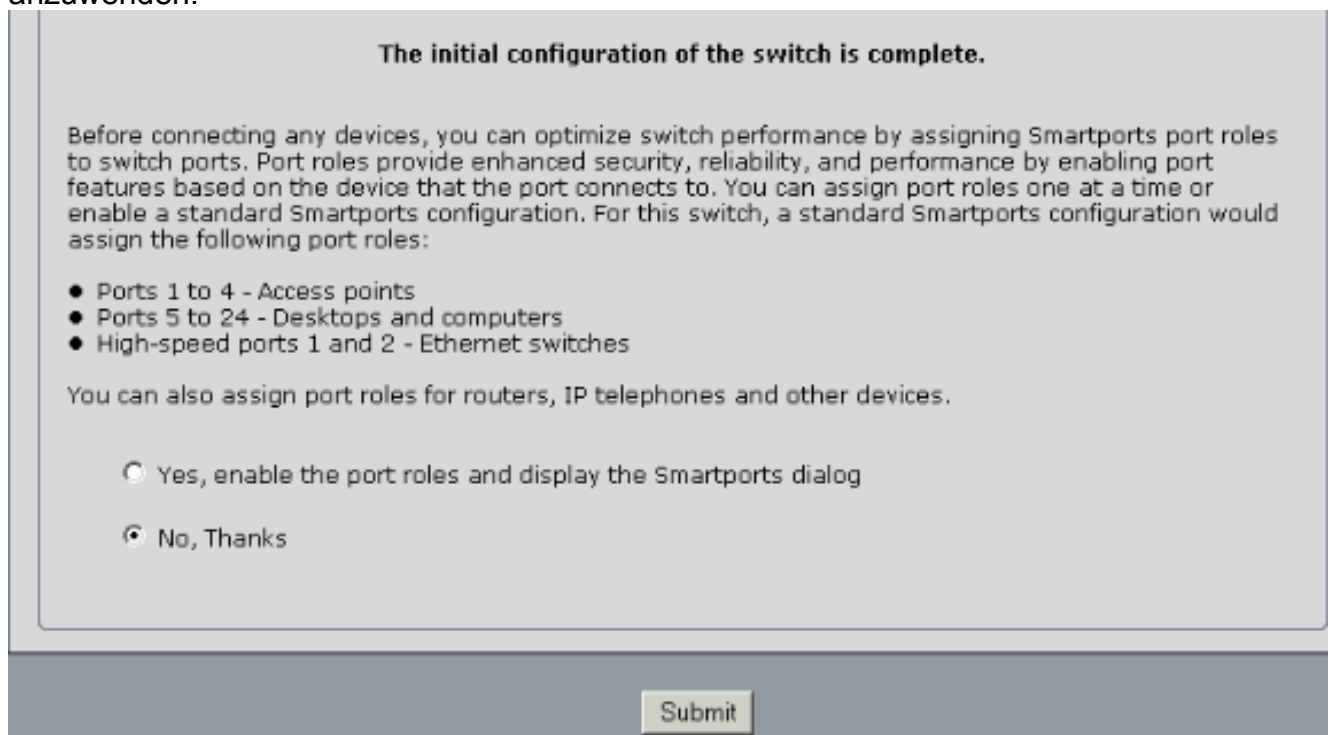
- 8. Geben Sie den konfigurierten Benutzernamen und das konfigurierte Kennwort ein, um mit der Konfiguration des Switches



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 both 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".

fortzufahren.

9. Im Dialogfeld "Smartports":Klicken Sie auf **Ja** und **Senden**, um die vordefinierten Portrollen zu akzeptieren. Das Fenster Smartports wird angezeigt. Hier können Sie die vordefinierten Rollen ändern oder neue Portrollen anwenden.Klicken Sie auf **Nein** und **Senden**, um die Smartports-Rollen selbst anzuwenden.



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. Starten Sie den Switch neu, ohne den Strom abzuschalten.

Restart / Reset

Restart the switch with its current settings.

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

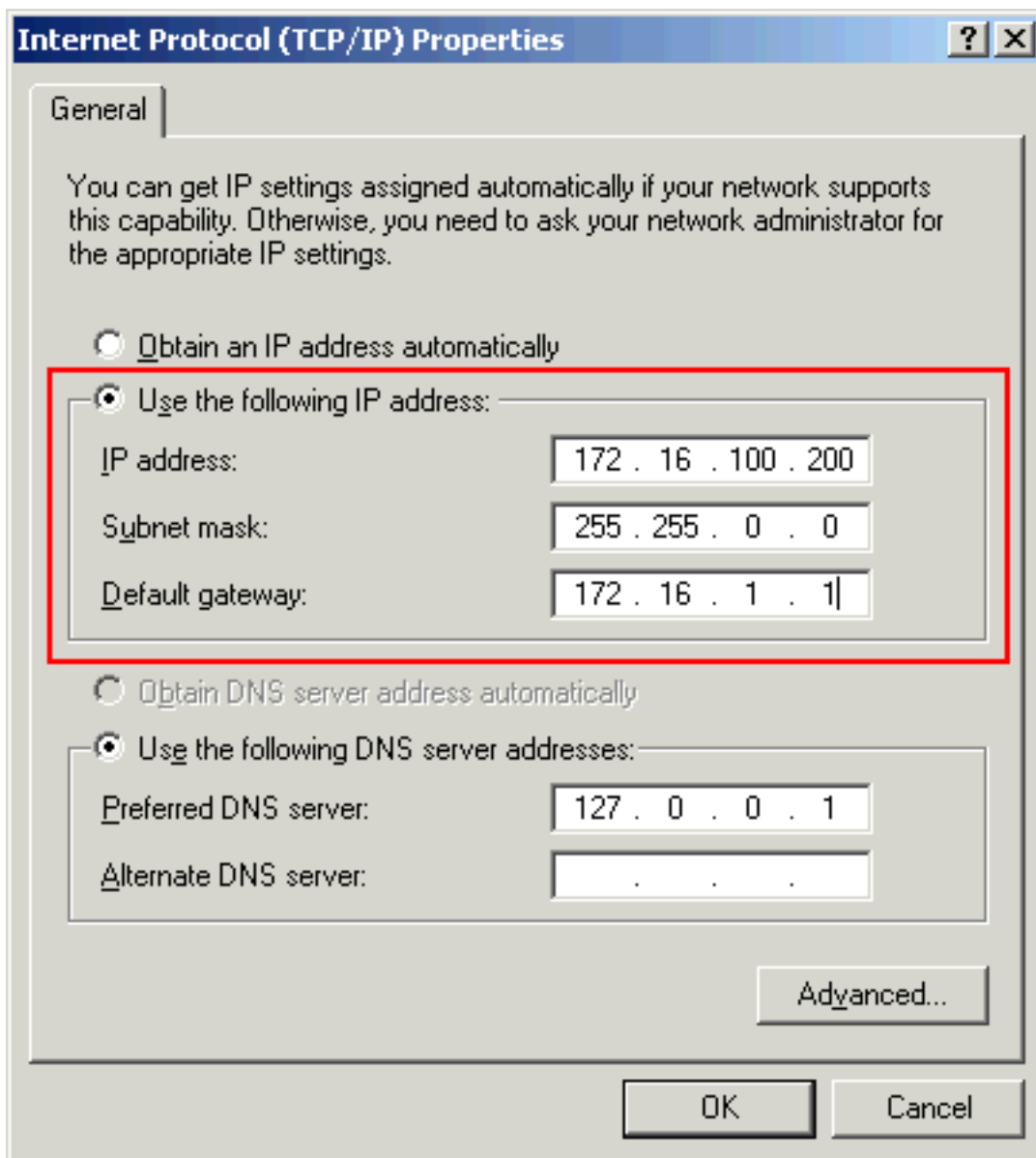
Submit Cancel

Der Switch wird automatisch in 60 Sekunden neu geladen. Ein Zähler zeigt die Zeit an, die für das erneute Laden verbleibt.

Restart / Reset

Device will be reloaded in 59 second(s).

11. Schließen Sie den Webbrowser, und konfigurieren Sie den LAN-Adapter mit einer IP-Adresse im gleichen Subnetz der neuen Management-Adresse des Switches



neu.

12. Wenn der Switch hochgefahren wird, öffnen Sie einen Webbrowser und gehen Sie zu http://<CE500_Management_IP_Address>. Beispiel: <http://172.16.100.100>. Hinweis: Sobald die Erstkonfiguration abgeschlossen ist, kann der Switch über jeden Switch-Port verwaltet werden, der für dasselbe VLAN wie die IP-Adresse des Managements konfiguriert ist.

Smartports

Smartport-Rollen

Bei den Smartports handelt es sich um vorkonfigurierte Switch-Ports, die vorab von Cisco empfohlene Netzwerkerweiterungen, Quality of Service (QoS) und Sicherheit bieten. Catalyst Express Switches der Serie 500 haben eine Reihe von SmartPort-Rollen. Jede Portrolle ist nur eine Konfigurationsvorlage. Mit diesen Vorlagen können Benutzer die grundlegenden Sicherheits-, Verfügbarkeits- und QoS-Funktionen konsistent und zuverlässig konfigurieren und dabei mit minimalem Aufwand und minimalem Fachwissen arbeiten. Smartport-Rollen vereinfachen die Konfiguration wichtiger Funktionen.

Die Portrollen basieren auf dem Gerätetyp, der mit den Switch-Ports verbunden werden soll. Beispielsweise ist die Desktop-Portrolle speziell für die Switch-Ports bestimmt, die mit Desktop- oder Laptop-PCs verbunden sind.

SmartPort-Rolle	Beschreibung
Desktop	<p>Legen Sie diese Funktion bei Ports an, die mit Desktop-Geräten verbunden sind, z. B. Desktop-PCs, Workstations, Notebook-PCs und andere Client-basierte Hosts.</p> <ul style="list-style-type: none"> • Optimiert für Desktop-Konnektivität • Konfigurierbare VLAN-Einstellung • Aktivierung der Port-Sicherheit zur Beschränkung des nicht autorisierten Zugriffs auf das Netzwerk
Switch	<p>Legen Sie diese Funktion bei Ports an, die mit anderen Switches verbunden sind.</p> <ul style="list-style-type: none"> • Konfiguriert als Uplink-Port zu einem Backbone-Switch für schnelle Konvergenz • Ermöglicht 802.1Q-Trunking • Konfigurierbares natives VLAN
Router	<p>Legen Sie diese Funktion bei Ports an, die mit WAN-Geräten verbunden sind, die mit dem Internet verbunden sind, z. B. Router und Layer-3-Switches mit Routing-Service-Funktionen, Firewalls oder VPN-Concentrators.</p> <ul style="list-style-type: none"> • Konfiguriert für die optimale Verbindung mit einem Router oder einer Firewall für WAN-Verbindungen • Ermöglicht 802.1Q-Trunking • Konfigurierbares natives VLAN
IP-Telefon+ Desktop	<p>Legen Sie diese Funktion bei Ports an, die mit IP-Telefonen verbunden sind. Ein Desktop-Gerät, z. B. ein PC, kann an das IP-Telefon angeschlossen werden. Sowohl das IP-Telefon als auch der angeschlossene PC haben über den Switch-Port Zugriff auf das Netzwerk und das Internet. Diese Rolle priorisiert Sprachdatenverkehr gegenüber Datenverkehr, um einen klaren Sprachempfang auf den IP-Telefonen sicherzustellen.</p> <ul style="list-style-type: none"> • Optimierte QoS für IP-Telefon- und Desktop-Konfigurationen • Sprachdatenverkehr wird über das Cisco-Voice-VLAN übertragen. • Konfigurierbares Daten-VLAN • QoS-Ebene gewährleistet Priorisierung des VoIP-Datenverkehrs • Aktivierung der Port-Sicherheit zur Beschränkung des nicht autorisierten

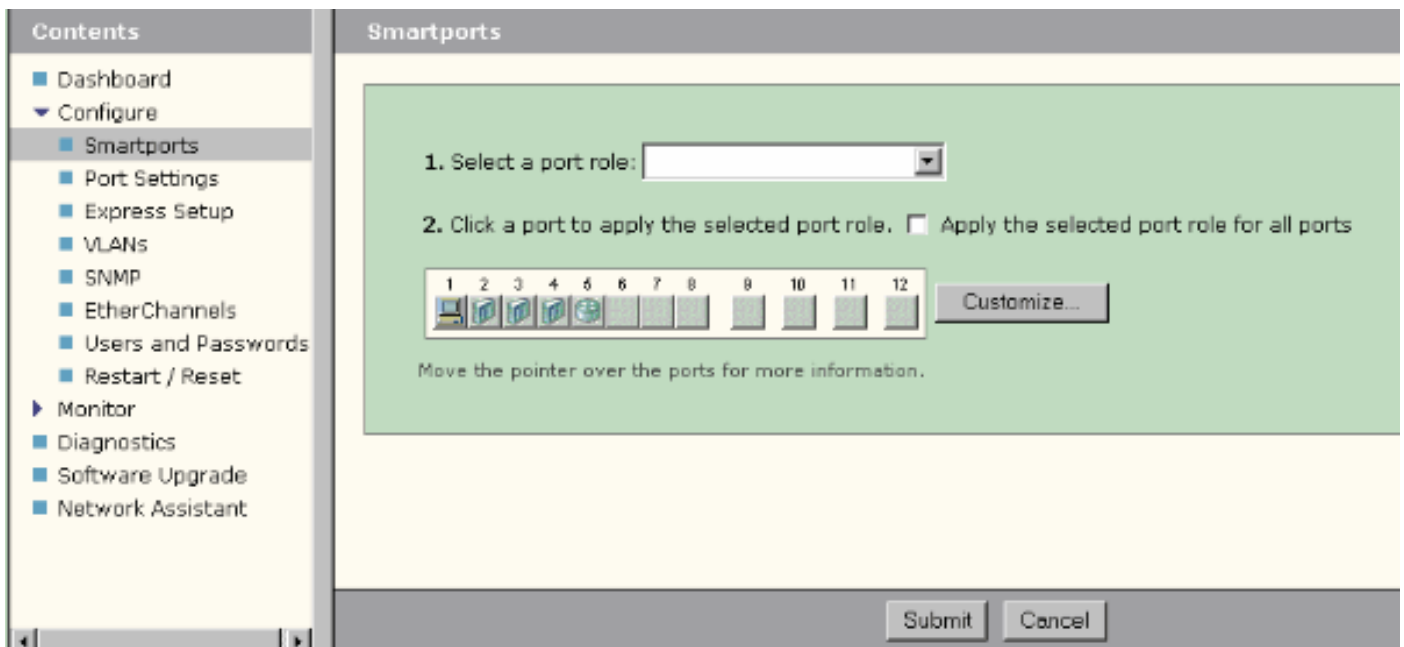
	Zugriffs auf das Netzwerk
Access Point	<p>Legen Sie diese Funktion bei Switch-Ports an, die eine Verbindung zu PoE- (Nicht-Power-over-Ethernet) und PoE-fähigen Wireless Access Points (APs) herstellen. Mit dem Access Point sind mobile Geräte verbunden, z. B. Wireless-Laptops.</p> <ul style="list-style-type: none"> • Konfiguriert für eine optimale Verbindung zu einem Wireless Access Point • Ermöglicht 802.1Q-Trunking • Konfigurierbares natives VLAN <p>Hinweis: Die Funktionen der Cisco Wireless Bridges ähneln denen eines Switches. Cisco empfiehlt daher die Switch-Smartport-Funktion für Wireless Bridges.</p>
Server	<p>Legen Sie diese Funktion bei Ports an, die mit Servern verbunden sind, die Netzwerkdienste bereitstellen, z. B. Exchange-Server, kollaborative Server, Terminalserver, Dateiserver, Dynamic Host Configuration Protocol (DHCP)-Server, IP Private Branch Exchange (PBX)-Server usw. Diese Rolle gilt für Gigabit- oder Nicht-Gigabit-Ports, abhängig vom anzuschließenden Servertyp.</p> <ul style="list-style-type: none"> • Konfigurierbares VLAN • Aktivierung der Port-Sicherheit zur Beschränkung des nicht autorisierten Zugriffs auf das Netzwerk <p>Diese Rolle priorisiert Serverdatenverkehr als vertrauenswürdig, kritisch, geschäftskritisch oder Standard, basierend auf der Funktion des Servers.</p> <ul style="list-style-type: none"> • Trusted (Vertrauenswürdig) - Zur Verwendung mit Cisco CallManager Express. Die gleiche QoS-Einstellung wie Voice (VoIP-Datenverkehr wird priorisiert). • Critical (Kritisch) - Für kritische Server mit QoS, die über dem Standardwert liegen. • Business: Die Standardeinstellung. QoS ist höher als Desktop-Internetdatenverkehr. • Standard - Für Server, die auf die gleiche Stufe wie der reguläre Internetdatenverkehr über Desktop-Systeme eingestellt sind.
Drucker	<p>Legen Sie diese Funktion bei Switchports an, die mit einem Drucker verbunden sind, z. B. einem Netzwerkdrucker oder einem externen</p>

	<p>Druckserver. Diese Rolle verhindert, dass der Druckerverkehr Sprache und wichtigen Datenverkehr beeinträchtigt.</p> <ul style="list-style-type: none"> • Die QoS-Einstellungen für Drucker entsprechen denen für Desktop, Access Point und Standardserver. • Konfigurierbares VLAN • Aktivierung der Port-Sicherheit zur Beschränkung des nicht autorisierten Zugriffs auf das Netzwerk
Gast	<p>Legen Sie diese Funktion bei Ports an, die mit Desktop-Geräten verbunden sind, und bei APs für den drahtlosen Gastzugriff an.</p> <ul style="list-style-type: none"> • Die Gäste haben Zugang zum Internet, aber nicht zum Unternehmensnetzwerk. • Alle Gast-Ports werden im Cisco Gast-VLAN platziert. • Die Port-Sicherheit ist aktiviert, um den nicht autorisierten Zugriff auf das Netzwerk zu beschränken.
Andere	<p>Legen Sie diese Funktion bei Switch-Ports an, wenn Sie keine spezielle Rolle für den Port zuweisen möchten. Diese Rolle kann für Verbindungen zu Gast- oder Besuchergeräten, Druckern, Desktops, Servern und IP-Telefonen verwendet werden. Sie ermöglicht eine flexible Anbindung nicht spezifizierter Geräte.</p> <ul style="list-style-type: none"> • Konfigurierbares VLAN • Keine Sicherheitsrichtlinie • Keine QoS-Richtlinie
Diagnose	<p>Kunden können Diagnosegeräte anschließen, um den Datenverkehr auf anderen Switches zu überwachen (kann nur mit Cisco Network Assistant konfiguriert werden).</p>

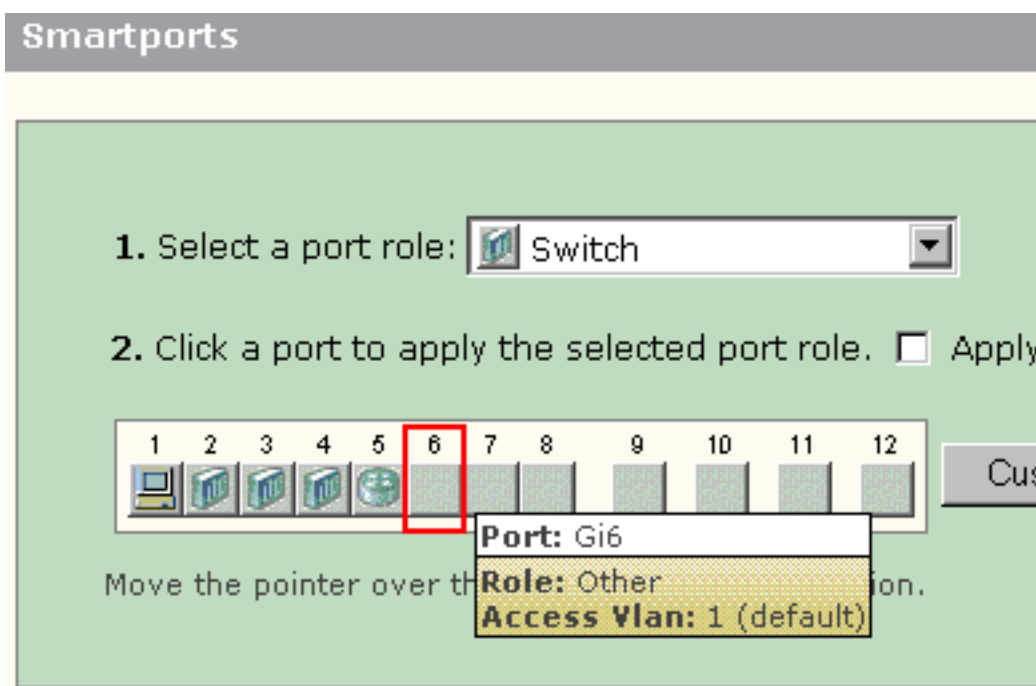
[Smartport-Rollen auf Ports anwenden](#)

Verwenden Sie das Fenster Smartports, um den Switch-Ports Portrollen zuzuweisen. Wählen Sie **Konfigurieren > Smartports** im Menü Gerätemanager aus, um dieses Fenster anzuzeigen. Sie

können auch in der Symbolleiste des Gerätemanagers auf **Smartports**  klicken.



Im Fenster Smartports können Sie sehen, welche Smartports-Rolle auf die einzelnen Ports angewendet wird. Bewegen Sie den Mauszeiger über einen Port, um dessen Portnummer, Smartports-Rolle und VLAN-ID (VLAN-Mitgliedschaft) anzuzeigen.



Bevor Sie Smartports verwenden, entscheiden Sie, welchen Switch-Port Sie für welchen Gerätetyp verwenden möchten. Sie können eine Smartports-Rolle auf einen [bestimmten Port](#) oder auf [alle Ports](#) des Switches anwenden.

[Einschränkungen](#)

- Es wird empfohlen, bestimmte Porteeinstellungen nicht zu ändern, nachdem Sie eine Smartports-Rolle auf einem Port aktiviert haben. Änderungen an den Port-Einstellungen können die Effektivität der Smartports-Rolle verändern.
- Wenden Sie die Desktop-Rolle nicht auf Ports an, die mit Switches, Routern oder APs verbunden sind.

- Der SmartPort-Rolle-**Switch** aktiviert automatisch 802.1Q-Trunking auf dem Port. Wenn ein Remote-Switch 802.1Q-Trunking nicht unterstützt oder das Trunking manuell ausgeschaltet wird, wird der Spanning-Tree-Status des Ports am Remote-Switch blockiert, um Typinkonsistenz zu vermeiden. Wenn der Remote-Switch die Root-Bridge ist, wechselt der Switch-Port nicht in den Blockierungsmodus. In diesem Fall ist der Trunk-Status des Switch-Ports an beiden Enden der Switches "ON" (An), aber es gibt keine Kommunikation zwischen den Switches über diese Ports. Auf dem Catalyst Express 500-Gerät werden keine Diagnosemeldungen angezeigt.**Ausgabe über Remote-Switch**

```
%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
```

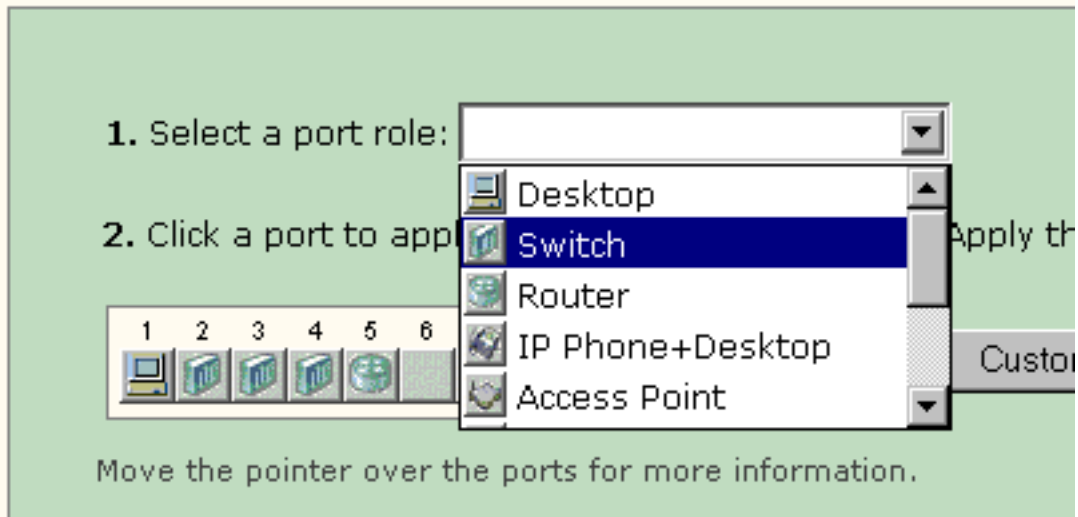
- Der SmartPort-Rolle-**Router** aktiviert automatisch 802.1Q-Trunking auf dem Port. Wenn die Hauptschnittstelle des Remote-Routers verwendet wird, stellen Sie sicher, dass die Schnittstelle des Routers Teil des nativen VLANs des Switch-Ports ist. Die Schnittstelle des Routers kann unterinteragiert werden, um Inter-VLAN-Routing für den Cisco Catalyst Express 500-Switch bereitzustellen. Konfigurationsdetails finden Sie im Abschnitt [Konfigurieren von Inter-VLAN-Routing mit einem Cisco Router](#) dieses Dokuments.
- Sie sollten über ein zusätzliches VLAN mit dem Namen **Cisco-Voice** (Groß- und Kleinschreibung beachten) verfügen, um die Portrolle **IP-Telefon+Desktop** Smartport auf die Ports anzuwenden.
- Sie sollten über ein zusätzliches VLAN mit dem Namen **Cisco-Guest** verfügen (Groß- und Kleinschreibung beachten), um die **Guest** Smartport-Rolle auf die Ports anzuwenden.
- Wenden Sie die Rolle Other nicht auf die Ports an, die mit einem Sniffer- oder Intrusion Detection-System verbunden sind.

[Anwenden einer Smartports-Rolle auf einen einzelnen Port](#)

Gehen Sie wie folgt vor, um eine Smartports-Rolle auf einen bestimmten Port anzuwenden:

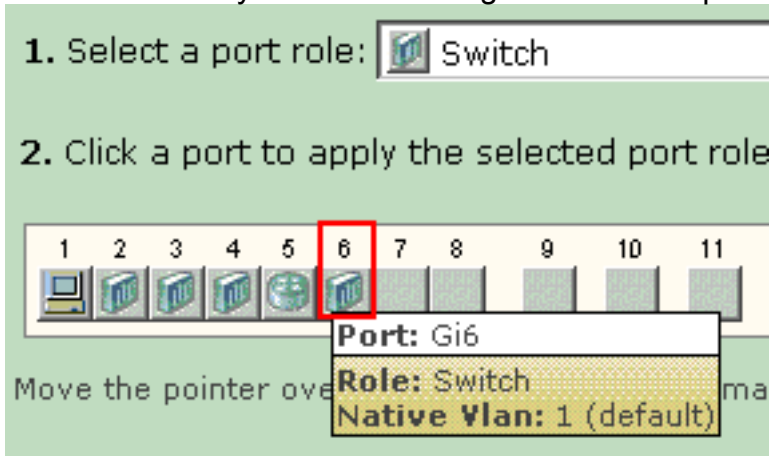
1. Wählen Sie eine Smartports-Rolle aus der Liste Wählen Sie eine Portrolle

Smartports



aus.

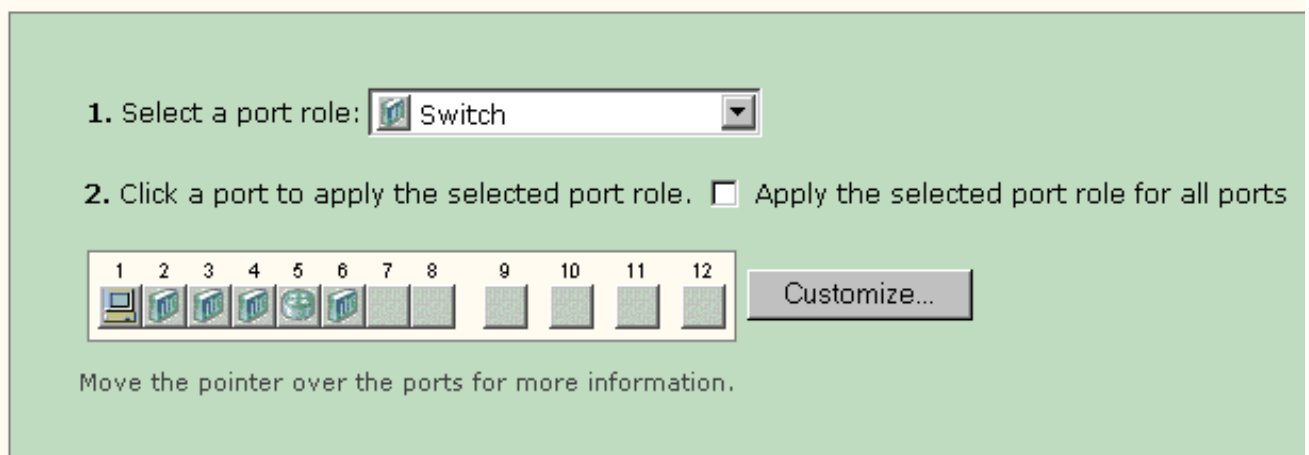
2. Klicken Sie auf den Port. Das Symbol für die ausgewählte Smartports-Rolle wird auf dem



Port angezeigt.

3. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Smartports



Submit

Cancel

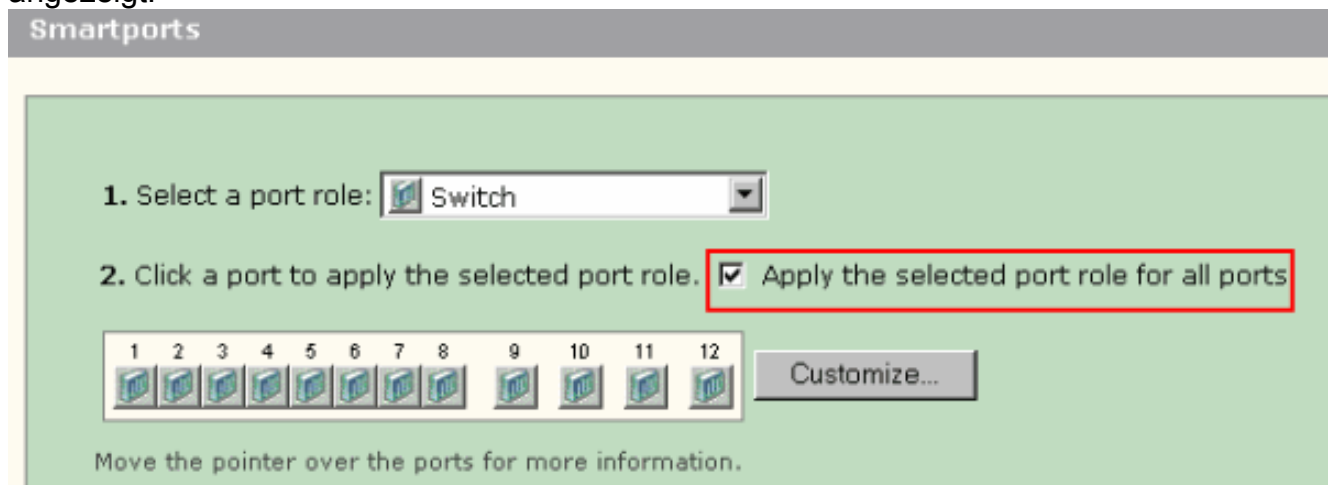
Gehen Sie wie folgt vor, um die auf einen Port angewendete Smartports-Rolle zu entfernen:

1. Wählen Sie **Andere** aus der Liste Wählen Sie eine Portrolle aus.
2. Klicken Sie auf den Port. Das Symbol Other (Andere) wird auf dem Port angezeigt.
3. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Anwenden einer Smartports-Rolle auf alle Ports

Gehen Sie wie folgt vor, um die ausgewählte Smartports-Rolle auf alle Ports anzuwenden:

1. Wählen Sie eine Smartports-Rolle aus der Liste Wählen Sie eine Portrolle aus.
2. Aktivieren Sie **die Option Gewählte Portrolle auf allen Ports übernehmen**. Das Symbol für die ausgewählte Smartports-Rolle wird an den Ports angezeigt.



3. Führen Sie die folgenden Schritte für alle Ports aus, die nicht mit der ausgewählten Portrolle angewendet werden sollten: Wählen Sie eine andere Smartports-Rolle aus der Liste Wählen Sie eine Portrolle aus. Klicken Sie auf den Port. Das Symbol für die ausgewählte Smartports-Rolle wird auf dem Port angezeigt.
4. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Gehen Sie wie folgt vor, um die auf alle Ports angewendete Smartports-Rolle zu entfernen:

1. Wählen Sie **Andere** aus der Liste Wählen Sie eine Portrolle aus.
2. Aktivieren Sie **die Option Gewählte Portrolle für alle Ports übernehmen**. Das Symbol Other (Andere) wird an den Ports angezeigt.
3. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Erstellen/Löschen von VLANs

VLAN-Typen

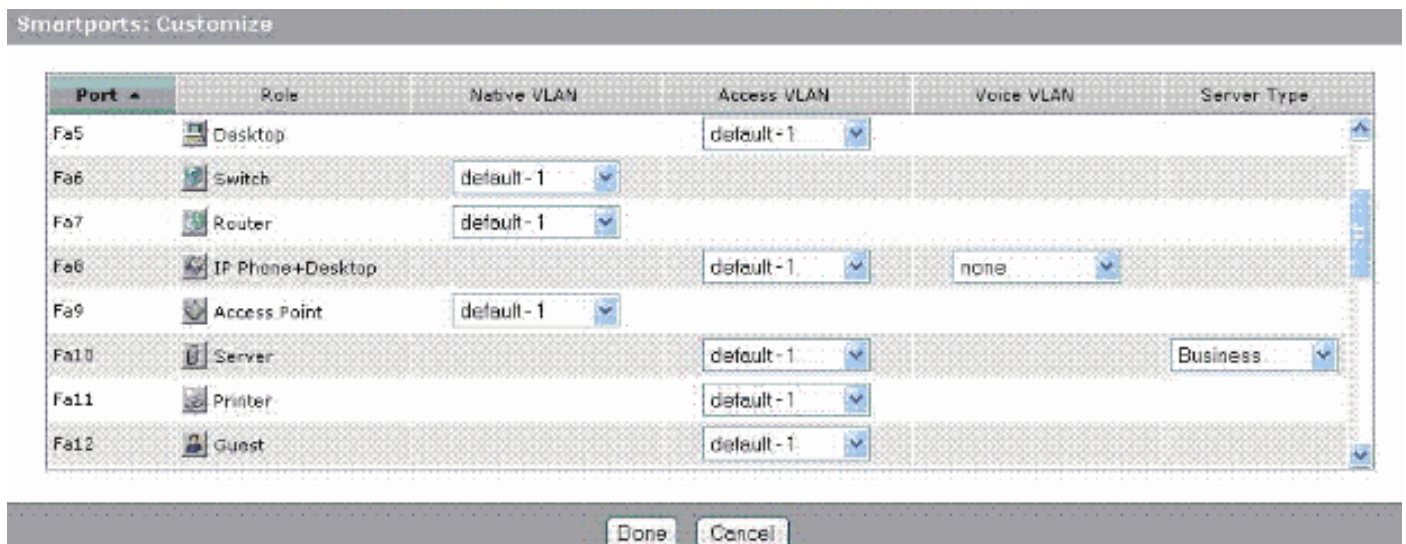
Der Switch wird mit einem Standard-VLAN ausgeliefert, zu dem alle Switch-Ports zunächst gehören. Der Switch unterstützt maximal 32 VLANs, einschließlich des Standard-VLANs. Je nach Größe und Anforderungen Ihres Netzwerks kann es ausreichen, nur das Standard-VLAN zu verwenden. Wir empfehlen Ihnen, zunächst Ihre VLAN-Anforderungen zu ermitteln, bevor Sie VLANs erstellen.

Hinweis: Cisco Catalyst Switches der Serie 500 arbeiten im VTP-Modus "Transparent". Das Erstellen, Ändern oder Löschen von VLANs auf diesem Switch hat keinen Einfluss auf die anderen Switches in der Domäne.

Dies hängt vom Gerätetyp ab, der mit dem Switch-Port verbunden ist:

- Ein Switch-Port mit einer dieser Portrollen kann nur zu einem Zugriffs-VLAN gehören: Desktop, IP-Telefon, Desktop, Drucker, Server, Gast, Andere. Das Zugriffs-VLAN stellt dem angeschlossenen Gerät den spezifischen Zugriff bereit, der für dieses VLAN vorgesehen ist.
- Ein Switch-Port mit einer dieser Portrollen kann Datenverkehr für alle auf dem Switch konfigurierten VLANs senden und empfangen, von denen eines als natives VLAN identifiziert werden kann: Switch, Router, Access Point. An diesem Port wird davon ausgegangen, dass der gesamte Datenverkehr, der ohne das explizit identifizierte VLAN empfangen oder gesendet wird, zum nativen VLAN gehört. Sowohl der Switch-Port als auch der Port des angeschlossenen Geräts müssen sich im selben nativen VLAN befinden.

Hinweis: Wählen Sie im Geräte-Manager **Configure > Smartports > Customize** aus, um die Portrollen und die zugehörigen VLANs anzuzeigen.



Wenn Ihr Netzwerk eine Trennung von Sprach- und Gastdatenverkehr bzw. eine Trennung vorsieht, müssen Sie zusätzliche VLANs erstellen. Wenn Sie zusätzliche VLANs auf dem Switch erstellen, auf dem IP-Telefon+Desktop und Voice Smartports installiert sind, müssen Sie außerdem folgende VLANs erstellen:

- **Cisco-Guest (Cisco-Guest):** Das VLAN, dem alle Ports zugewiesen werden, die die Guest-Portrolle übernehmen. Dieses VLAN stellt sicher, dass der gesamte Gast- und Besucherverkehr vom restlichen Netzwerkverkehr und den übrigen Ressourcen getrennt wird. Ports mit **Guest** Smartport-Rollen sollten diesem VLAN zugewiesen werden.
- **Cisco-Voice:** Das VLAN, dem alle Ports zugewiesen werden, die die IP-Telefon+Desktop-Portrolle übernehmen, muss zugewiesen werden. Dieses VLAN stellt sicher, dass der gesamte Sprachverkehr über eine bessere QoS verfügt und nicht mit dem Datenverkehr gemischt wird. Das Sprach-VLAN von Ports mit **IP Phone+Desktop** Smartport-Rollen sollte diesem VLAN zugewiesen werden.

Verwenden Sie das Fenster VLANs, um VLANs zu erstellen und zu löschen. Wählen Sie **Configure > VLANs** im Menü Geräte-Manager aus, um dieses Fenster anzuzeigen.

1. Gehen Sie wie folgt vor, um ein VLAN zu erstellen:

2. Klicken Sie im Fenster VLANs auf **Erstellen**.

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

3. Geben Sie den Namen und die ID für das VLAN ein.

4. Klicken Sie auf

Fertig.

VLAN Name:

VLAN ID:

5. Wiederholen Sie die Schritte 1 bis 3, bis Sie die erforderlichen VLANs erstellen.

6. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

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

Hinweis: Wenn Sie über Ports mit der IP-Telefon+Desktop-Rolle verfügen, müssen Sie das Cisco-Voice-VLAN erstellen. Wenn Sie Ports mit der Guest-Portrolle haben, müssen Sie das Cisco-Guest VLAN erstellen. Wenn Sie VLANs ohne Cisco-Voice- und Cisco-Guest-VLANs erstellen und auf **Senden** klicken, wird diese Fehlermeldung angezeigt.



Gehen Sie wie folgt vor, um VLAN(s) zu löschen:

1. Aktivieren Sie das Kontrollkästchen oben in der Spalte "Löschen", um alle VLANs auszuwählen, oder aktivieren Sie das Kontrollkästchen für ein oder mehrere spezifische VLANs.

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. Klicken Sie auf **Senden**, um die Änderungen zu speichern. Klicken Sie im Popup-Fenster "VLAN-Bestätigung löschen" auf **OK**.

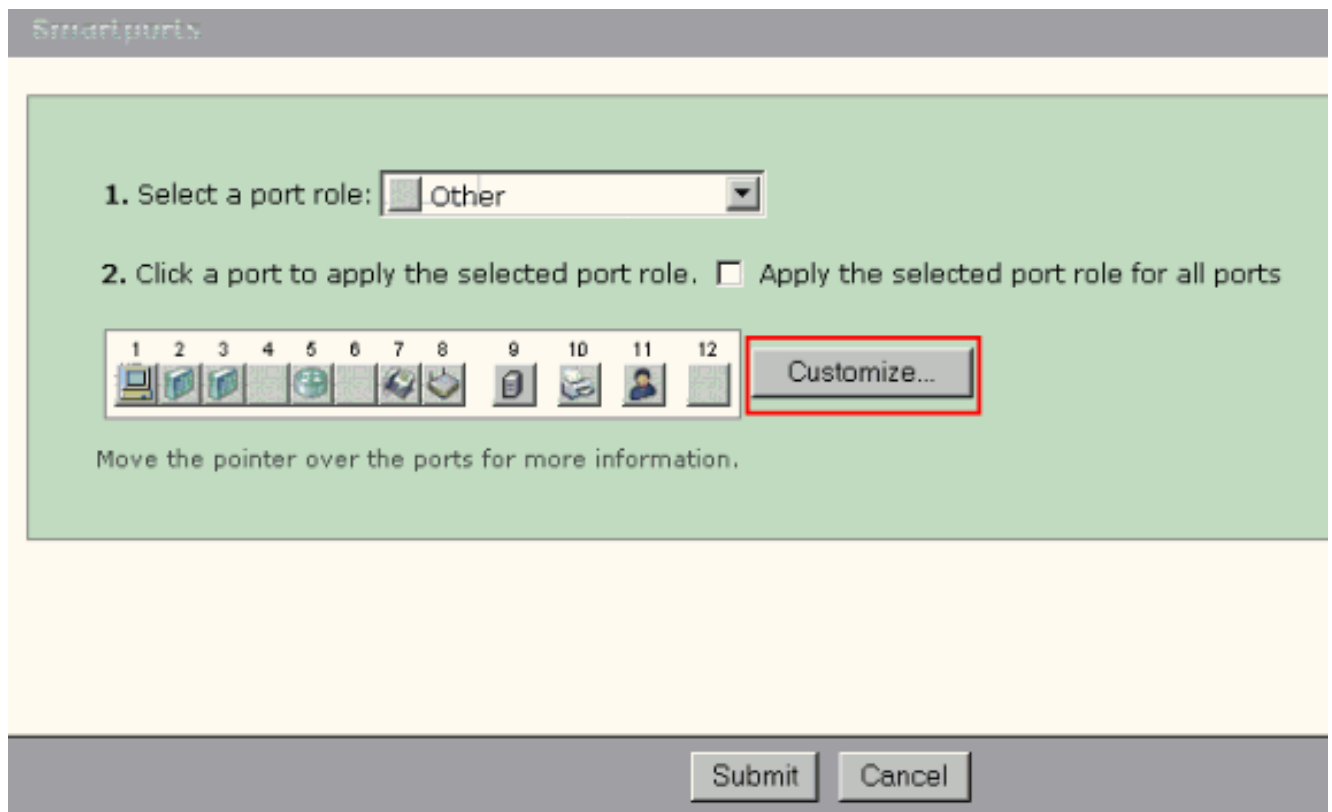
VLAN-Mitgliedschaft ändern

Bestimmte VLAN-Mitgliedschaften können für die Ports geändert werden, die zu diesen Smartport-Rollen gehören:

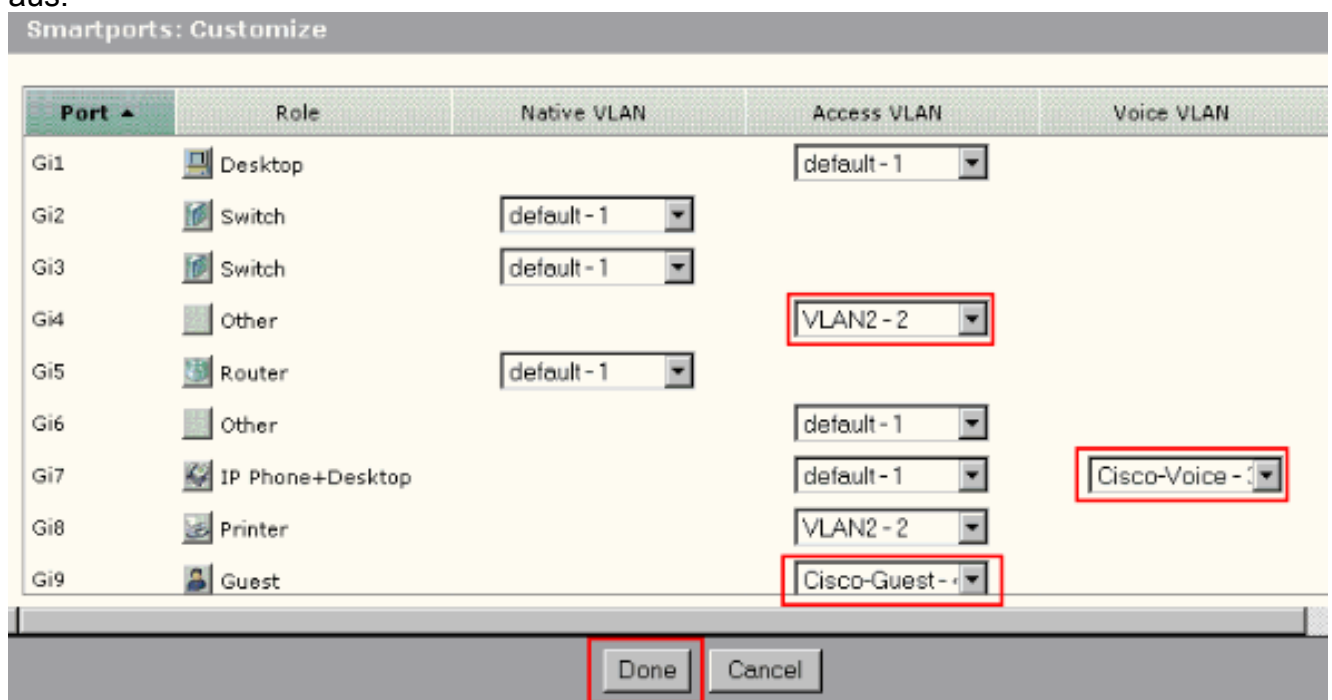
- **Natives VLAN** - Switch, Router und Access Point
- **Zugriffs-VLAN** - Desktop, IP-Telefon+Desktop, Server, Drucker, Gast und andere **Hinweis:** Das Zugriffs-VLAN für die Gastrolle sollte das Cisco-Guest VLAN sein.
- **Sprach-VLAN** - IP-Telefon+Desktop Das Sprach-VLAN sollte nur das Cisco-Voice-VLAN sein.

Verwenden Sie das Fenster Smartports anpassen, um VLANs Ports zuzuweisen. Wählen Sie **Konfigurieren > Smartports** im Menü Geräte-Manager aus, um dieses Fenster anzuzeigen.

1. Klicken Sie im Fenster Smartports auf **Anpassen**.



2. Wählen Sie die entsprechenden VLAN(s) für jeden Port aus.



3. Klicken Sie auf **Fertig**.

4. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Konfigurieren von EtherChannels

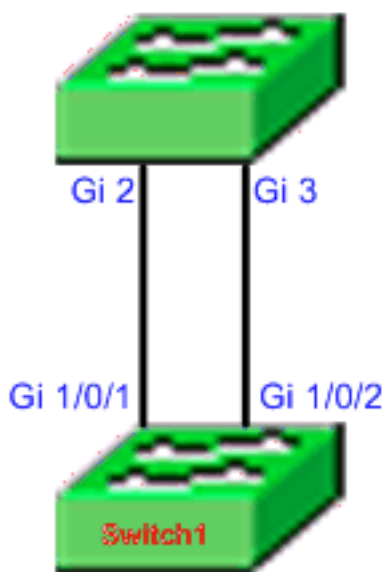
Ein EtherChannel ist eine Gruppe von zwei oder mehr Fast Ethernet- oder Gigabit Ethernet-Switch-Ports, die in einer einzigen logischen Verbindung gebündelt sind und eine Verbindung mit höherer Bandbreite zwischen zwei Switches schaffen. Der Switch unterstützt bis zu sechs EtherChannels.

Alle Ports in einem EtherChannel müssen die gleichen Merkmale aufweisen:

- Alle Ports sind entweder 10/100-Ports oder alle 10/100/1000-Ports. Sie können eine Mischung aus 10/100- und 10/100/1000-Ports nicht in einem EtherChannel gruppieren.
- Alle Ports verfügen über die gleichen Einstellungen für Geschwindigkeit und Duplexmodus.
- Alle Ports werden mit der Smartports Switch-Portrolle angewendet und gehören zum gleichen VLAN.

Gehen Sie wie folgt vor, um EtherChannels zwischen einem Cisco Catalyst Express 500 und einem anderen Switch zu erstellen:

Cisco Catalyst Express CE500G-12TC Switch



Cisco Catalyst 3750 Series Switch

1. Wählen Sie im Geräte-Manager des Cisco Catalyst Express 500-Switches **Configure > EtherChannels** aus, um das EtherChannels-Fenster anzuzeigen.
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die Channel-Gruppen-ID ein.
4. Wählen Sie das Channel Protocol (Modus) für die Liste Modus aus. **Hinweis:** Der Catalyst Express 500-Switch unterstützt zwei Modi, die als LACP und Static (Statisch) bezeichnet werden. Konfigurieren Sie den Remote-Switch entsprechend dem gewählten Modus.
5. Klicken Sie auf die Kontrollkästchen für die Ports, die Teil des Kanals sein sollen.
6. Klicken Sie auf **Fertig** und dann auf **Senden**, um die Änderungen zu speichern.

EtherChannels: Create

Group [1-6]:

Mode:

Port ▲	In Group
Gi2	<input checked="" type="checkbox"/>
Gi3	<input checked="" type="checkbox"/>

7. Wenn Sie für das Aushandeln des Kanals das LACP-Protokoll ausgewählt haben, konfigurieren Sie den Remote-Switch wie folgt:

```
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
```

Wenn Sie den Kanal statisch konfigurieren möchten, konfigurieren Sie den Remote-Switch wie folgt:

```
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
```

Überprüfen

Öffnen Sie das Fenster **Configure > EtherChannels**, um den Status des erstellten EtherChannels zu überprüfen. Der Status sollte als "In Use" (In Verwendung) angezeigt werden. Andernfalls können Sie eine Diagnose für die Ports durchführen, um das Problem zu ermitteln.

EtherChannels

Group ▲	Ports	Status
1	Gi2, Gi3	In Use

Geben Sie den Befehl **show etherchannel summary** im Cisco 3750 Switch ein, um den Status der EtherChannel-Konfiguration zu überprüfen. Im Feld Protokoll in der Ausgabe wird **LACP** angezeigt, wenn dieser zum Aushandeln des Kanals verwendet wird (leer oder anderweitig).

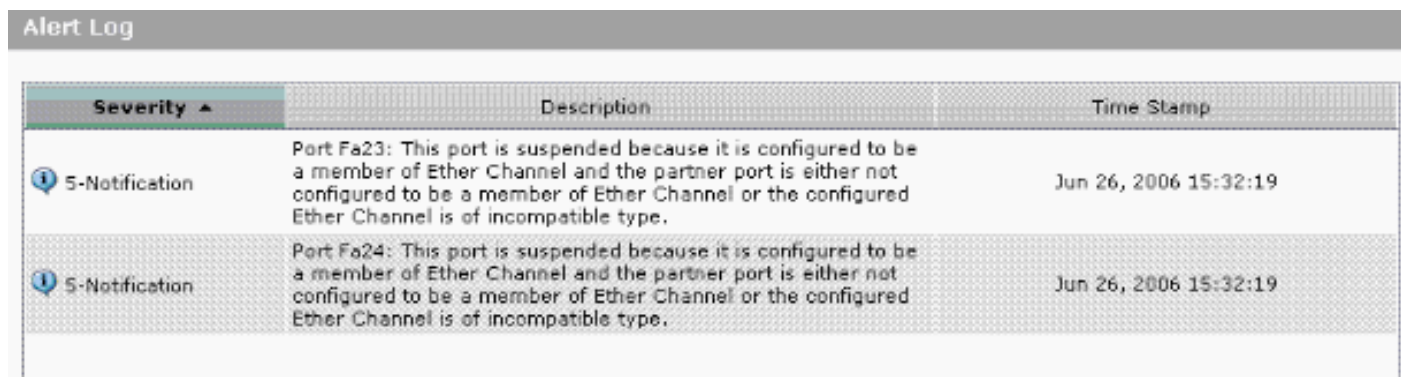
```
Switch#show etherchannel summary
```

```
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)
```

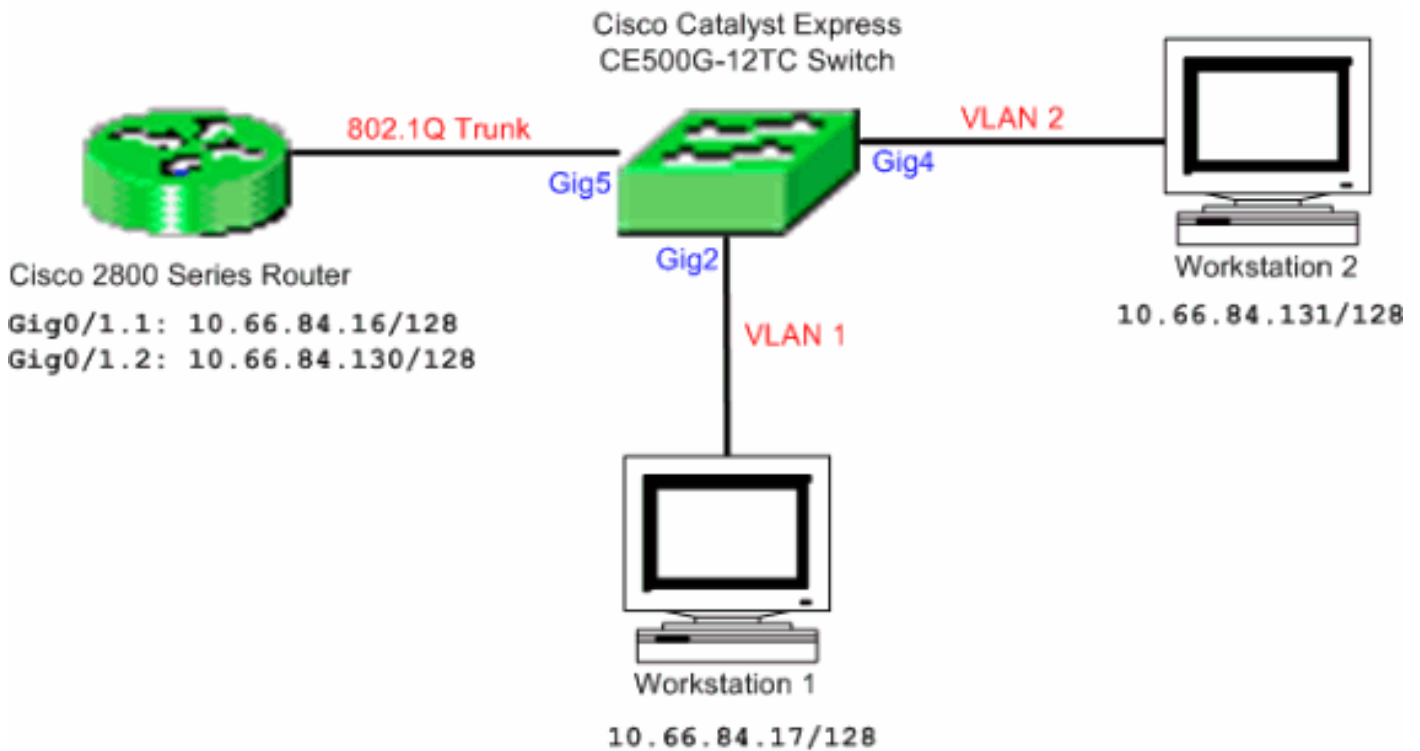
Sie können auch das Catalyst 500-Switch-Protokoll von **Monitor > Alert Log** im Geräte-Manager sehen. Dieses Beispiel zeigt die EtherChannel-Fehlermeldung aufgrund der EtherChannel-Fehlkonfiguration auf dem Remote-Switch.



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

[Konfigurieren von Inter-VLAN-Routing mit einem Cisco Router](#)

Netzwerkdiagramm



Hinweis: Bei der Beispielkonfiguration wird der Cisco Router der Serie 2800 verwendet. Dies kann durch jeden Cisco Router ersetzt werden, der IEEE 802.1Q-Trunking unterstützt.

Gehen Sie wie folgt vor, um Inter-VLAN-Routing mit einem Cisco Router zu konfigurieren:

1. Gehen Sie wie folgt vor, um den Cisco Catalyst Express 500-Switch zu konfigurieren: Wenden Sie die Desktop Smartport-Rolle auf die Ports Gig2 und Gig4 an. Das Konfigurationsverfahren finden Sie im Abschnitt [Smartport-Rollen auf Ports anwenden](#) in diesem Dokument. Wenden Sie die Router Smartport-Rolle auf Port Gig5 an. Wenden Sie die entsprechenden VLAN-IDs auf die Ports an. Weisen Sie VLAN 1 als Zugriffs-VLAN für den Port Gig2 zu. Weisen Sie VLAN 2 als Zugriffs-VLAN für den Port Gig4 zu. Weisen Sie VLAN 1 als natives VLAN für Port Gig5 zu. Das Konfigurationsverfahren finden Sie im Abschnitt [VLAN-Mitgliedschaft ändern](#) in diesem Dokument.

2. Konfigurieren Sie den Cisco Router der 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
```

Überprüfen

Wählen Sie **Monitor > Portstatus** im Geräte-Manager aus, um den Trunk-Status des Switch-Ports auf dem Catalyst Express 500 Switch anzuzeigen.

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

Überprüfen Sie, ob der Ping von Workstation 1 zu Workstation 2 erfolgreich verläuft.

```
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
```

Führen Sie eine Ablaufverfolgung aus, um den Pfad für die Kommunikation zwischen Workstation 1 und Workstation 2 zu überprüfen.

```
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.
```

[SPAN \(Switched Port Analyzer\) konfigurieren](#)

Die SPAN-Funktion (Switched Port Analyzer), die auch als Portspiegelung oder Portüberwachung bezeichnet wird, wählt Netzwerkverkehr zur Analyse durch einen Netzwerkanalyst aus. Der Netzwerkanalysator kann ein Cisco SwitchProbe-Gerät oder eine andere Remote Monitoring (RMON)-Prüfung sein. Der Switch unterstützt nur das lokale SPAN und kein Remote-SPAN.

Der Zielport sollte mit der SmartPort-Funktion Diagnostics konfiguriert werden. Dies kann nur mit der Cisco Network Assistant-Software durchgeführt werden. Informationen zur Konfiguration des Catalyst Express 500-Switches zur [Überwachung des](#) Datenverkehrs finden Sie im [SPAN auf Catalyst Express 500](#).

[Setzen Sie den Catalyst Express 500-Switch auf die werkseitigen Standardeinstellungen zurück.](#)

Wenn Sie eine Verbindung zum Geräte-Manager des Switches haben und den Switch auf die Werkseinstellungen zurücksetzen und die aktuelle Cisco IOS-Systemsoftware beibehalten möchten, lesen Sie den Abschnitt [Zurücksetzen des Switches mithilfe des Geräte-Managers Zurücksetzen der Catalyst Express Switches der Serie 500 auf die werkseitigen Standardeinstellungen](#).

Wenn Sie keine Verbindung zum Gerätemanager des Switches haben und den Switch auf die Werkseinstellungen zurücksetzen möchten, lesen Sie den Abschnitt [Zurücksetzen des Switches bei Nichtverfügbarkeit des Gerätemanagers](#) im Abschnitt [Zurücksetzen der Catalyst Express Switches der Serie 500 auf die werkseitigen Standardeinstellungen](#).

Weitere Informationen zum Wiederherstellungsverfahren finden Sie im Abschnitt [Wiederherstellen der Switch-Software](#) im [Benutzerhandbuch für Catalyst Express 500 Switches - Fehlerbehebung](#).

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Einführungsinformationen für Catalyst Express 500 Switches](#)
- [Benutzerhandbuch für Catalyst Express 500 Switches](#)
- [Grundlegendes zum EtherChannel-Lastenausgleich und zur Redundanz auf Catalyst-Switches](#)
- [Konfigurieren von Inter-VLAN-Routing und ISL/802.1Q-Trunking auf einem Catalyst 2900XL/3500XL/2950-Switch mithilfe eines externen Routers](#)
- [Produktsupport für Switches](#)
- [Unterstützung der LAN Switching-Technologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)