

# Catalyst Express versie 500 Series Switches Configuratievoorbeld

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configuratie eerste Switch](#)

[Smartports](#)

[Smartport Roles](#)

[Slimme rollen op poorten toepassen](#)

[Beperkingen](#)

[Een Smartports-rol op één poort toepassen](#)

[Een slimme rol op alle poorten toepassen](#)

[VLAN's maken/verwijderen](#)

[VLAN-typen](#)

[VLAN-lidmaatschap wijzigen](#)

[EtherChannel configureren](#)

[InterVLAN-routing met een Cisco router](#)

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

[Zet de Catalyst Express 500 Switch terug op fabrieksinstellingen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## **[Inleiding](#)**

Dit document beschrijft de procedure die u gebruikt om Cisco Catalyst Express 500 Series switches te configureren voor slimme poortrollen, VLAN's, EtherChannel, Switch Port Analyzer (SPAN) en routing tussen VLAN's uit te voeren met de Cisco Catalyst Express 500 Series switch.

## **[Voorwaarden](#)**

### **[Vereisten](#)**

Cisco raadt kennis van de volgende onderwerpen aan:

- EtherChannel

- Inter-VLAN-routing
- SPAN

Configureer de switch van de Cisco Catalyst 500 Series met de initiële netwerkinstellingen zoals vermeld in het gedeelte [Configuration voor de eerste switch](#) van dit document.

U kunt het gegevensblad voor Cisco Catalyst 500 Series switches zien om meer over de verschillende modellen en de ondersteunde functies te weten te komen in [Cisco Catalyst Express 500 Series Switches](#).

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst Express versie 12.2(25)FY
- Cisco 2800 router die IEEE 802.1Q Trunk-insluiting ondersteunt.
- Cisco Catalyst 3750 switches die 802.1Q Trunk-insluiting ondersteunen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies](#).

## Configuratie eerste Switch

Voltooi deze stappen om een eerste instelling van de switch uit te voeren. Raadpleeg de [Introductiegids voor de Catalyst Express 500 Switches](#) voor meer informatie over de configuratieprocedure.

1. Zorg ervoor dat er geen verbinding is met de switch.
2. Macht de switch.
3. Wacht tot het LED-indicatielampje groen knippert.
4. Klik op **Instellen**. Een LED-poort op de switch begint groen te knipperen.
5. Wanneer een switch-poort op LED groen knippert, sluit u uw PC aan op die poort. De LAN-adapter van deze PC moet worden geconfigureerd om het IP-adres via DHCP te krijgen. De LEDs op de PC en de schakelaar knipperen groen terwijl de switch de verbinding vormt (dit duurt ongeveer een minuut).
6. Open een webbrowser. Voltooi deze stappen als de browser de GUI niet automatisch opzuigt: Geef het **ipfig** bevel uit om de dynamische adrestoewijzing te bekijken.

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

Windows 2000 IP Configuration

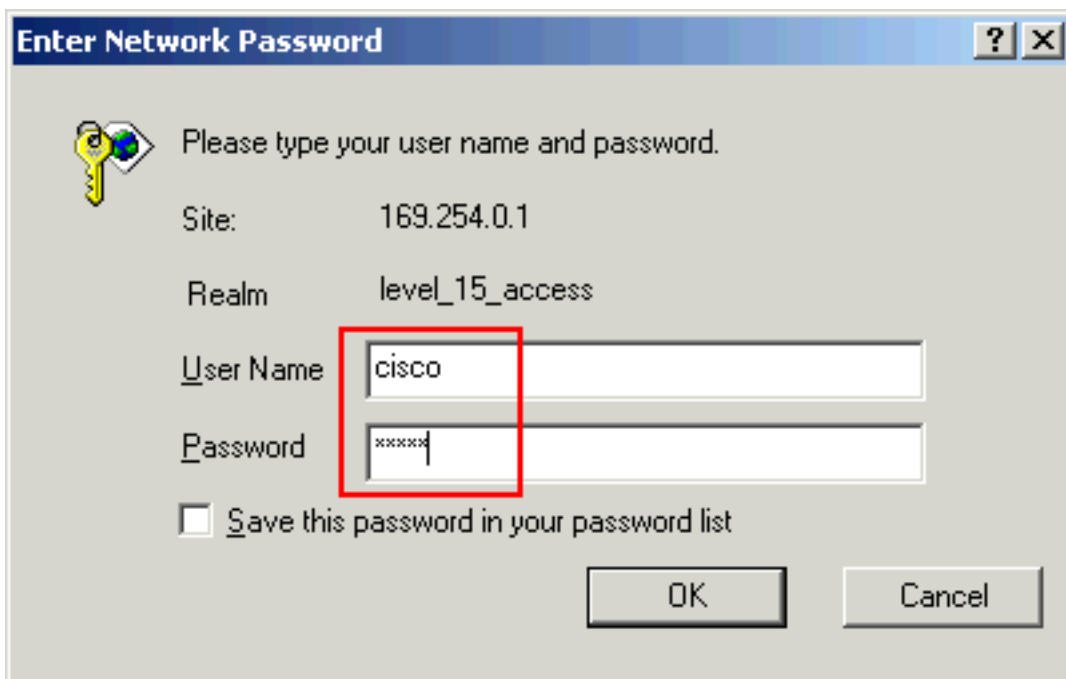
Ethernet adapter Local Area Connection:

    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
```

De switch stelt zijn beheeradres in als de standaardgateway voor de LAN-adapterkaart van de pc. **Opmerking:** Voor Cisco IOS Software FY Series releases is het IP-adres van het beheer 10.0.0.1. Voor Cisco IOS **SEG**-series releases is het IP-adres 169.254.0.1. Ga vanuit de browser naar het vermelde IP-adres. Bijvoorbeeld, <http://169.254.0.1>.

- 7. Voer de netwerkinstellingen in en selecteer Optionele instellingen (indien nodig). Klik op **Indienen** om wijzigingen op te slaan en de basisconfiguratie te voltooien.

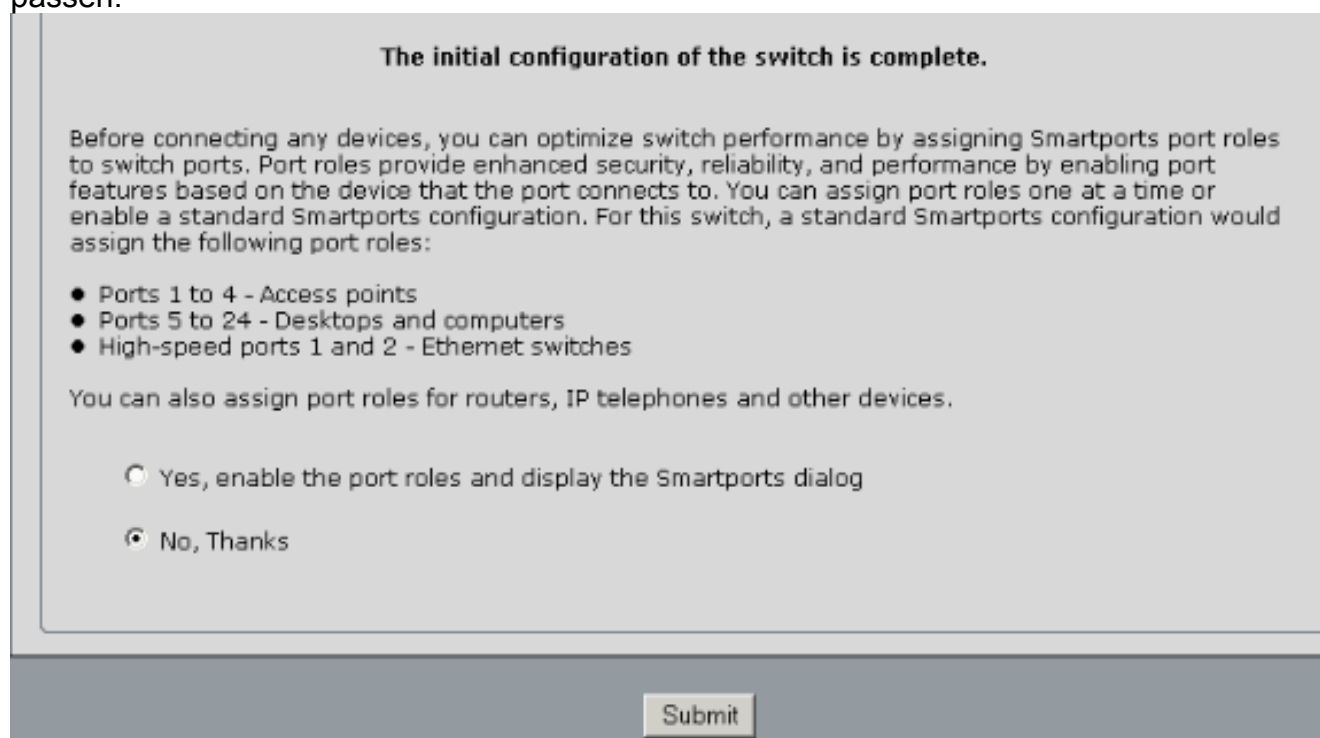
- 8. Voer de ingestelde naam en het wachtwoord in om door te gaan met het configureren van de



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

switch.

9. U vindt in het dialoogvenster Smartports het volgende: Klik op **Ja** en **Indienen** om de vooraf gedefinieerde poortrollen te aanvaarden. Het venster Smartports verschijnt. Hier kunt u de vooraf gedefinieerde rollen wijzigen of nieuwe poortrollen toepassen. Klik op **Nee** en **Indienen** om de Smartports rollen zelf toe te passen.



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. Start de switch opnieuw zonder de stroom uit te schakelen.

Restart / Reset

Restart the switch with its current settings.

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

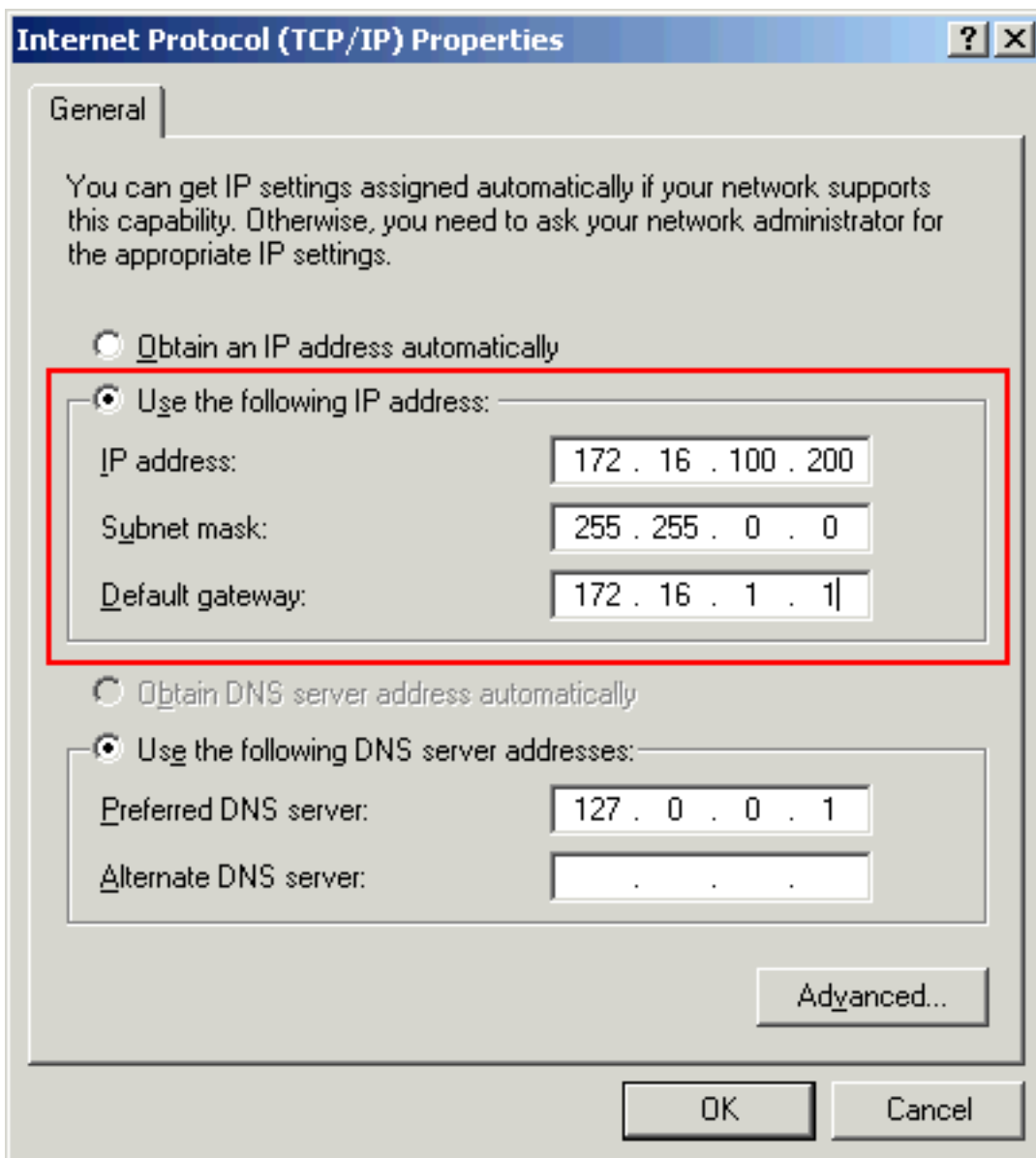
Submit Cancel

De switch wordt automatisch opnieuw geladen in 60 seconden. Een teller geeft de tijd weer die voor het opnieuw laden overblijft.

Restart / Reset

Device will be reloaded in 59 second(s).

11. Sluit de webbrowser en pas de LAN adapter aan met een IP adres binnen hetzelfde subtype van het nieuwe beheeradres van de



switch.

12. Wanneer de switch verschijnt, opent u een webbrowser en gaat u naar [http://<CE500\\_Management\\_IP\\_Address>](http://<CE500_Management_IP_Address>). Bijvoorbeeld, <http://172.16.100.100>. **Opmerking:** Zodra de eerste configuratie is voltooid, kan de switch worden bestuurd via een willekeurige verbindingsoort die is ingesteld voor hetzelfde VLAN als dat van het IP-adres van het beheer.

## [martports](#)

### [Smartport Roles](#)

De Smartports zijn vooraf geconfigureerd switch-poorten die vooraf ingestelde Cisco-aanbevolen netwerkverbeteringen, QoS-kwaliteit (Quality of Service) en beveiliging bieden. Catalyst Express 500 Series switches hebben een aantal slimme rollen. Elke poortrol is gewoon een configuratiesjabloon. Met deze sjablonen kunnen gebruikers consistent en betrouwbaar essentiële security, beschikbare en QoS-functies met minimale inspanning en expertise configureren. Slimme rollen vereenvoudigen de configuratie van kritieke functies.

De poortrollen zijn gebaseerd op het type apparaten dat op de poorten van de switch moet worden aangesloten. Bijvoorbeeld, de rol van de Desktop poort is specifiek voor de poorten van de switch die op desktop of laptop PCs worden aangesloten.

martretpo rt	Beschrijving
Desktop	<p>Pas deze rol toe op poorten die zijn aangesloten op desktop apparaten, zoals desktop PCs, werkstations, notebook PCs, en andere op client gebaseerde hosts.</p> <ul style="list-style-type: none"> <li>• Geoptimaliseerd voor desktopconnectiviteit</li> <li>• Configureerbare VLAN-instelling</li> <li>• Poortbeveiliging is ingeschakeld om onbevoegde toegang tot het netwerk te beperken</li> </ul>
Switch	<p>Pas deze rol op havens toe die op andere switches worden aangesloten.</p> <ul style="list-style-type: none"> <li>• Als uplink-poort naar een backbone-switch configureren voor snelle convergentie</li> <li>• Maakt 802.1Q trunking mogelijk</li> <li>• Configureerbaar natuurlijk VLAN</li> </ul>
router	<p>Pas deze rol op poorten toe die worden aangesloten op WAN-apparaten die op het internet aangesloten zijn, zoals routers en Layer 3-switches met routingservicemogelijkheden, firewalls of VPN-concentrators.</p> <ul style="list-style-type: none"> <li>• Configureerbaar voor optimale verbinding met een router of firewall voor WAN-connectiviteit</li> <li>• Maakt 802.1Q trunking mogelijk</li> <li>• Configureerbaar natuurlijk VLAN</li> </ul>
IP- telefoon+ Desktop	<p>Pas deze rol op havens toe die op IP telefoons worden aangesloten. Een desktop apparaat, zoals een PC, kan op de IP telefoon worden aangesloten. Zowel de IP-telefoon als de aangesloten pc hebben toegang tot het netwerk en internet via de switch poort. Deze rol prioriteert spraakverkeer boven gegevensverkeer om duidelijke spraakontvangst op de IP-telefoons te verzekeren.</p> <ul style="list-style-type: none"> <li>• Geoptimaliseerde QoS voor IP-telefoon + desktopconfiguraties</li> <li>• Spraakverkeer wordt op Cisco-Voice VLAN geplaatst</li> <li>• Configureerbare gegevens van VLAN</li> <li>• QoS-niveau garandeert dat VoIP-verkeer (Voice-over-IP) voorrang krijgt</li> <li>• Poortbeveiliging is ingeschakeld om onbevoegde toegang tot het netwerk te</li> </ul>

	beperken
Access point	<p>Pas deze rol op switch poorten toe die verbinden met non-Power over Ethernet (PoE) en PoE-enabled draadloze access points (APs). Aangesloten op AP zijn mobiele apparaten, zoals draadloze laptop PC's.</p> <ul style="list-style-type: none"> <li>• geconfigureerd voor optimale aansluiting op een draadloos access point</li> <li>• Maakt 802.1Q trunking mogelijk</li> <li>• Configureerbaar natuurlijk VLAN</li> </ul> <p><b>Opmerking:</b> De functionaliteit van Cisco draadloze bruggen lijkt meer op die van een switch. Dus, Cisco adviseert de <b>Switch</b> smartport rol voor Draadloze bruggen.</p>
Server	<p>Pas deze rol toe op poorten die zijn aangesloten op servers die netwerkservices leveren, zoals Exchange-servers, collaboratieve servers, terminal servers, bestandsservers, Dynamic Host Configuration Protocol (DHCP)-servers, IP Private Branch (PBX)-servers, enzovoort. Deze rol is voor Gigabit of niet-Gigabit poorten, gebaseerd op het servertype dat moet worden aangesloten.</p> <ul style="list-style-type: none"> <li>• Configureerbaar VLAN</li> <li>• Poortbeveiliging is ingeschakeld om onbevoegde toegang tot het netwerk te beperken</li> </ul> <p>Deze rol prioriteert serververkeer als vertrouwd, kritisch, zakelijk of standaard, gebaseerd op de functie van de server.</p> <ul style="list-style-type: none"> <li>• <b>Trusted</b>-voor gebruik met Cisco CallManager Express. Dezelfde QoS-instelling als spraak (VoIP-verkeer wordt als prioriteit geselecteerd).</li> <li>• <b>Cruciaal</b>: voor kritische servers met QoS hoger dan standaard.</li> <li>• <b>Business</b>-de standaardinstelling. QoS is hoger dan het desktop internetverkeer.</li> <li>• <b>Standaard</b>—voor servers op hetzelfde niveau als voor het normale desktop internetverkeer.</li> </ul>
Printerprinter	<p>Pas deze rol op de havens van de switch toe die met een printer, zoals een netwerkprinter of een externe drukserver verbinden. Deze rol voorkomt printer verkeer van invloed op spraak- en kritische gegevensverkeer.</p> <ul style="list-style-type: none"> <li>• QoS-instellingen voor printer zijn hetzelfde als desktop-, access point- en standaardserver</li> </ul>

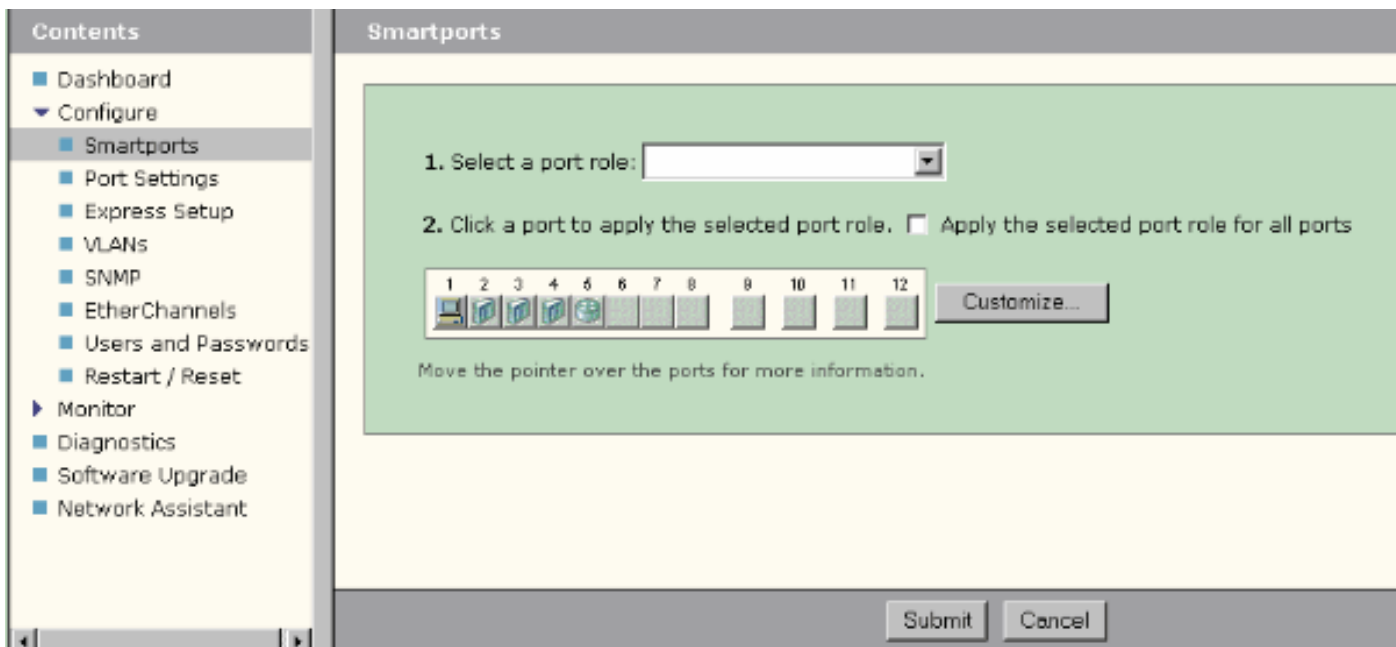


	<ul style="list-style-type: none"> <li>• Configureerbaar VLAN</li> <li>• Poortbeveiliging is ingeschakeld om onbevoegde toegang tot het netwerk te beperken</li> </ul>
Guest	<p>Pas deze rol op havens toe die op desktop apparaten en op APs worden aangesloten om de gast draadloze toegang te verlenen.</p> <ul style="list-style-type: none"> <li>• Burgers hebben toegang tot internet, maar niet tot het bedrijfsnetwerk.</li> <li>• Alle gastpoorten worden op Cisco-Gast VLAN geplaatst.</li> <li>• Poortbeveiliging is ingeschakeld om de toegang door onbevoegden tot het netwerk te beperken.</li> </ul>
Other (Overig)	<p>Pas deze rol op de havens van de switch toe als u geen specialistische rol op de haven wilt toewijzen. Deze rol kan worden gebruikt op verbindingen met gast of bezoekers apparaten, printers, desktops, servers, en IP telefoons. Het maakt flexibele connectiviteit van niet-gespecificeerde apparaten mogelijk.</p> <ul style="list-style-type: none"> <li>• Configureerbaar VLAN</li> <li>• Geen veiligheidsbeleid</li> <li>• Geen QoS-beleid</li> </ul>
diagnostiek	<p>Klanten kunnen diagnostische apparaten aansluiten om verkeer op andere switches te controleren (kunnen worden geconfigureerd met alleen Cisco Network Assistant).</p>

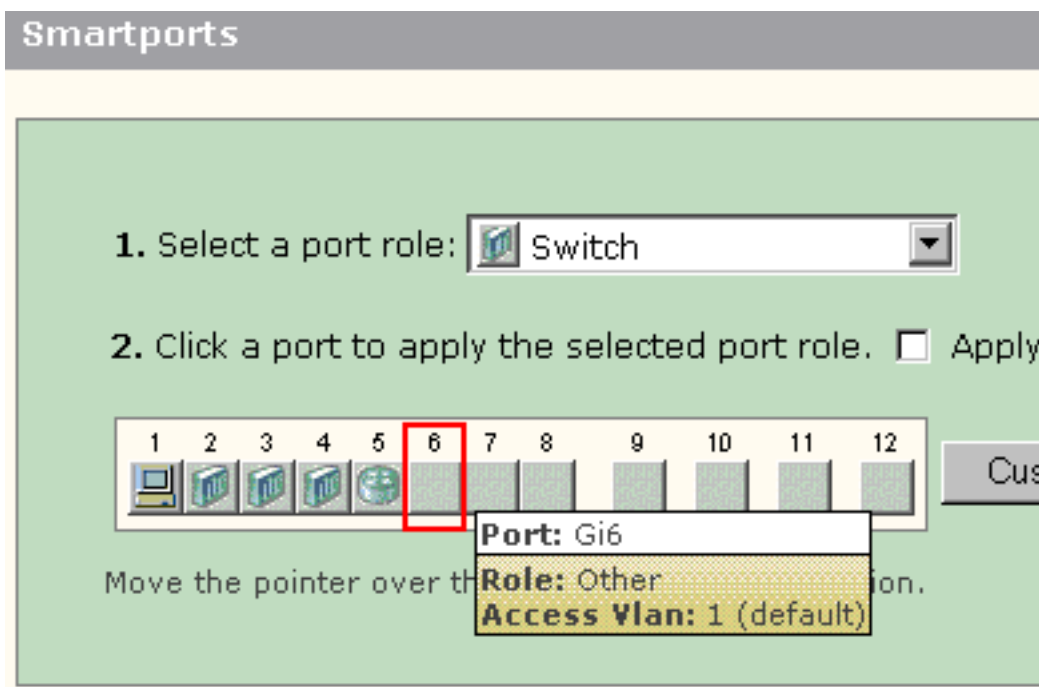
## [Slimme rollen op poorten toepassen](#)

Gebruik het venster Smartports om poortrollen op de poorten van de switch toe te passen. Selecteer **Configureren > Smartports** in het menu apparaatbeheer om dit venster weer te geven. U

kunt ook op **Smartports**  klikken in de werkbalk van de apparaatbeheer.



Vanuit het Smartports venster kunt u zien welke Smartports rol op elke poort wordt toegepast. Verplaats de wijzer over een haven om zijn havenaantal, Smartports rol, en VLAN ID (het lidmaatschap van VLAN) te tonen.



Bespaar voordat u Smartports gebruikt de switch die u van plan bent aan te sluiten op welk apparaattype. U kunt een Smartports rol toepassen op een [specifieke haven](#) of op [alle havens](#) op de switch.

## [Beperkingen](#)

- Wij raden u aan om bepaalde poortinstellingen niet te wijzigen nadat u een Smartports rol op een poort hebt ingeschakeld. Elke wijziging van de haveninstelling kan de effectiviteit van de Smartports rol veranderen.
- Pas de desktoprol niet toe op poorten die zijn aangesloten op switches, routers of AP's.
- Met de **Switch** Martport role kan automatisch 802.1Q trunking in de poort worden uitgevoerd.

Als een switch op afstand geen 802.1Q trunking ondersteunt of als de trunking handmatig wordt uitgeschakeld, dan blokkeert de overspannende boomstatus van de poort op de afstandsbediening om inconsistentie van het type te voorkomen. Als de switch op afstand de root-brug is, gaat de switch poort niet naar de blokkeringsmodus. In dit geval is de status van de boomstam van de switch aan beide uiteinden van de switches, maar er is geen communicatie tussen de switches door deze havens. Er worden geen diagnostische berichten weergegeven op Catalyst Express 500 apparaat. **Uitvoer van de afstandsbediening**

```
%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
```

- De marthport rol **Router** maakt automatisch 802.1Q trunking op de poort mogelijk. Als de belangrijkste interface van de afstandsrouter wordt gebruikt, zorg er dan voor dat de interface van de router deel uitmaakt van het inheemse VLAN van de switch poort. De interface van de router kan worden subinterfaces om de routing tussen VLAN's te bieden voor de Cisco Catalyst Express 500-switch. Zie het [configureren van InterVLAN-routing met een Cisco-routersectie](#) van dit document voor configuratiegegevens.
- U dient een extra VLAN met de naam **Cisco-Voice** (hoofdlettergevoelig) te hebben om de marthport-rol van **IP Phone+Desktop** op de poorten toe te passen.
- U dient een extra VLAN te hebben met de naam **Cisco-Guest** (hoofdlettergevoelig) om de **Guest** Smartport-rol op de poorten toe te passen.
- Pas de andere rol niet toe op de poorten die zijn aangesloten op apparaten voor snuifdetectie of inbraakdetectiesysteem.

## [Een Smartports-rol op één poort toepassen](#)

Voltooi deze stappen om een Smartports rol toe te passen op een specifieke haven:

1. Kies een Smartports rol uit de Select a port role

## Smartports

1. Select a port role:

2. Click a port to apply the selected port role

1 2 3 4 5 6

Desktop  
Switch  
Router  
IP Phone+Desktop  
Access Point

Apply the selected port role to all ports

Customize...

Move the pointer over the ports for more information.

list.

2. Klik op de port. Het pictogram voor de geselecteerde Smartports rol verschijnt op de

1. Select a port role: Switch

2. Click a port to apply the selected port role

1 2 3 4 5 6 7 8 9 10 11

Port: Gi6  
Role: Switch  
Native Vlan: 1 (default)

Move the pointer over the ports for more information.

poort.

3. Klik op **Inzenden** om de wijzigingen op te slaan.

## Smartports

1. Select a port role: Switch

2. Click a port to apply the selected port role.  Apply the selected port role for all ports

1 2 3 4 5 6 7 8 9 10 11 12

Customize...

Move the pointer over the ports for more information.

Submit

Cancel

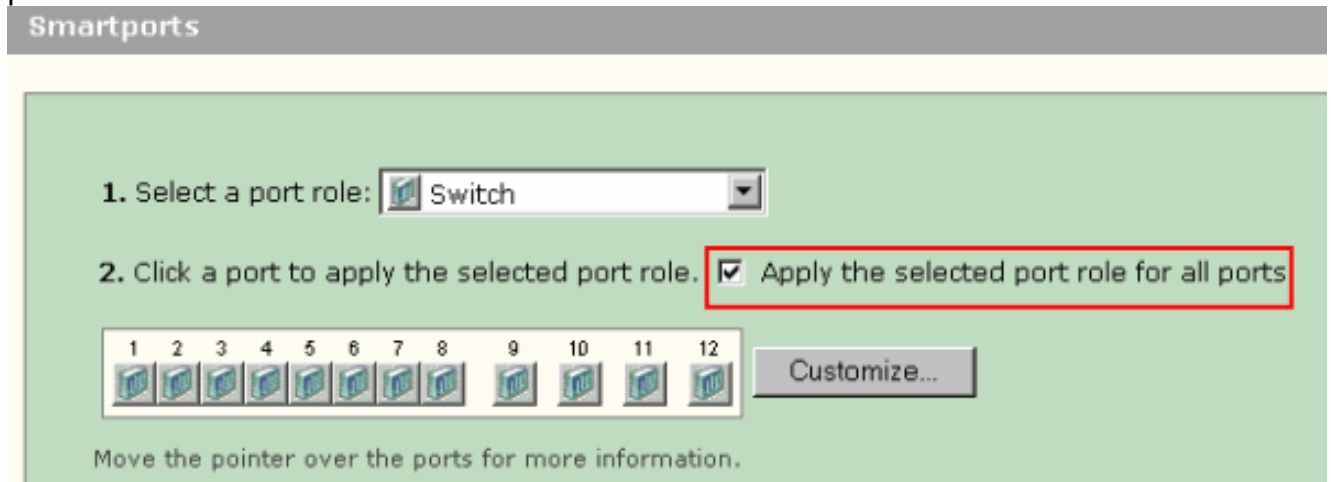
Voltooi deze stappen om de Smartports rol op een haven te verwijderen:

1. Kies **Andere** uit de Selecteer een lijst van de havenrol.
2. Klik op de poort. Het andere pictogram verschijnt in de poort.
3. Klik op **Inzenden** om de wijzigingen op te slaan.

## Een slimme rol op alle poorten toepassen

Voltooi deze stappen om de geselecteerde Smartports rol op alle poorten toe te passen:

1. Kies een Smartports rol uit de Select a port role list.
2. Controleer **de geselecteerde poortrol op alle poorten**. Het pictogram voor de geselecteerde Smartports rol verschijnt op de poorten.



3. Voltooi deze stappen voor elke haven(s) die niet met de geselecteerde havenrol mag worden toegepast: Kies een andere Smartports rol uit de Select a port role list. Klik op de poort. Het pictogram voor de geselecteerde Smartports rol verschijnt op de poort.
4. Klik op **Inzenden** om de wijzigingen op te slaan.

Voltooi deze stappen om de Smartports-rol die op alle poorten van toepassing is, te verwijderen:

1. Kies **Andere** uit de Selecteer een lijst van de havenrol.
2. Controleer **de geselecteerde poortrol voor alle poorten**. Het andere pictogram verschijnt in de havens.
3. Klik op **Inzenden** om de wijzigingen op te slaan.

## VLAN's maken/verwijderen

### VLAN-typen

De switch scheppen met een standaard VLAN waartoe alle switch havens aanvankelijk behoren. De switch ondersteunt een maximum van 32 VLAN's, inclusief het standaard VLAN. Alleen het standaard VLAN kan op basis van de grootte en vereisten van uw netwerk toereikend zijn. We raden u aan eerst uw VLAN-behoefte te bepalen voordat u VLAN's maakt.

**Opmerking:** Cisco Catalyst 500 Series switches werken in VTP Transparent Mode. De creatie, wijziging of schrapping van VLAN die op deze switch wordt gedaan heeft geen invloed op de andere switches in het domein.

Dit is afhankelijk van het type apparaat dat met de poort van de switch is verbonden:

- Een switch poort die met één van deze poortrollen wordt toegepast kan slechts tot een toegang VLAN behoren: Desktop, IP-telefoon, Printer, Server, Guest, Other (Overig). Het toegangs VLAN voorziet het aangesloten apparaat van de specifieke toegang die voor dat VLAN wordt ontworpen.
- Een switch poort die met één van deze poortrollen wordt toegepast kan verkeer voor alle VLAN's verzenden en ontvangen die op de switch zijn geconfigureerd, waarvan één als inheems VLAN kan worden geïdentificeerd: Switch, router, Access point. Op deze poort wordt elk verkeer dat zonder het expliciet geïdentificeerde VLAN wordt ontvangen of verzonden verondersteld tot het inheemse VLAN te behoren. Zowel de switch poort als de aangesloten apparaatpoort moet in hetzelfde VLAN zijn.

**Opmerking:** Selecteer **Configureren > Smartports > Pas aan** in Apparaatbeheer om de poortrollen en bijbehorende VLAN's te zien.

Smartports: Customize

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

Done Cancel

Als uw netwerk vereist dat u of zowel stem als gastverkeer scheidt, moet u extra VLAN's creëren. Als u extra VLAN's maakt in de switch waar u IP Phone+Desktop en Smartports voor de spraak hebt, moet u deze VLAN's ook maken:

- **Cisco-Guest**-Het VLAN waarop alle poorten die met de Guest poortrol worden toegepast, moeten worden toegewezen. Dit VLAN waarborgt dat al uw gast en bezoekersverkeer van de rest van uw netwerkverkeer en middelen gescheiden is. Poorten met **Guest** SmartPort-rollen moeten aan dit VLAN worden toegewezen.
- **Cisco-Voice**-Het VLAN waarop alle poorten die met de IP Phone+Desktop poortrol worden toegepast, moeten worden toegewezen. Dit VLAN waarborgt dat al het spraakverkeer betere QoS heeft en niet gemengd is met gegevensverkeer. De stem VLAN van poorten met **IP Phone+Desktop** rollen zou aan dit VLAN moeten worden toegewezen.

Gebruik het venster VLAN's om VLAN's te maken en te verwijderen. Selecteer **Configureren > VLAN's** in het menu Apparaatbeheer om dit venster weer te geven.

1. Voltooi deze stappen om een VLAN te maken:
2. Klik op **Maken** in het venster van VLAN's.

VLANs

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

3. Voer de naam en de ID voor het VLAN in.

4. Klik op  
**Klaar.**

VLAN: Create

VLAN Name:

VLAN ID:

5. Herhaal stappen 1 door 3 tot u de gewenste VLAN's maakt.

6. Klik op **Inzenden** om de wijzigingen op te slaan.

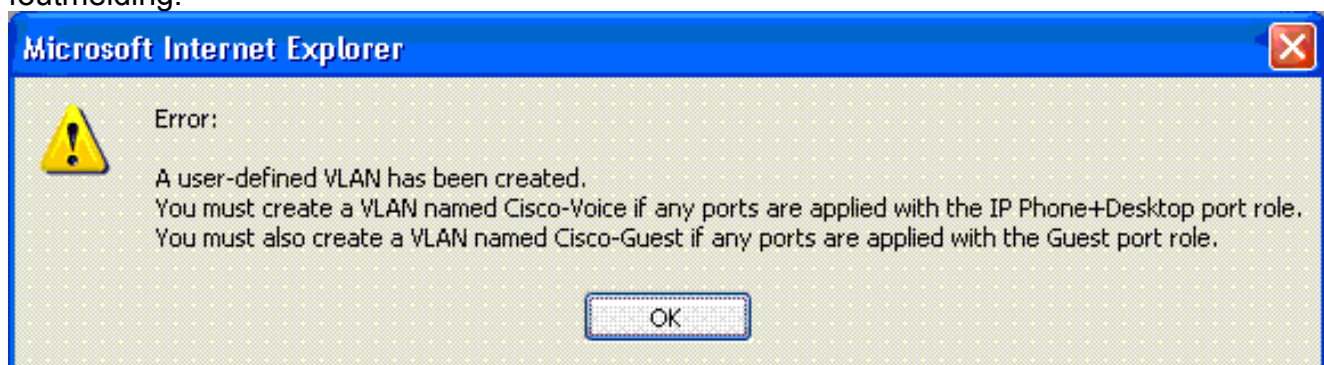
VLANS

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

**Opmerking:** Als u poorten hebt met de IP Phone+Desktop rol, moet u Cisco-Voice VLAN maken. Als u poorten hebt met de Guest poortrol, moet u het Cisco-Guest VLAN maken. Als u VLAN's maakt zonder Cisco-Voice- en Cisco-Guest VLAN's en u op **Inzenden** klikt, verschijnt deze foutmelding.



Voltooi deze stappen om VLAN(s) te verwijderen:

1. Controleer het aankruisvakje aan de bovenzijde van de kolom Verwijderen om alle VLAN's te selecteren of controleer het aankruisvakje voor een of meer specifieke VLAN's.



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. Klik op **Inzenden** om de wijzigingen op te slaan. Klik op **OK** in het pop-upvenster Bevestiging van VLAN verwijderen.

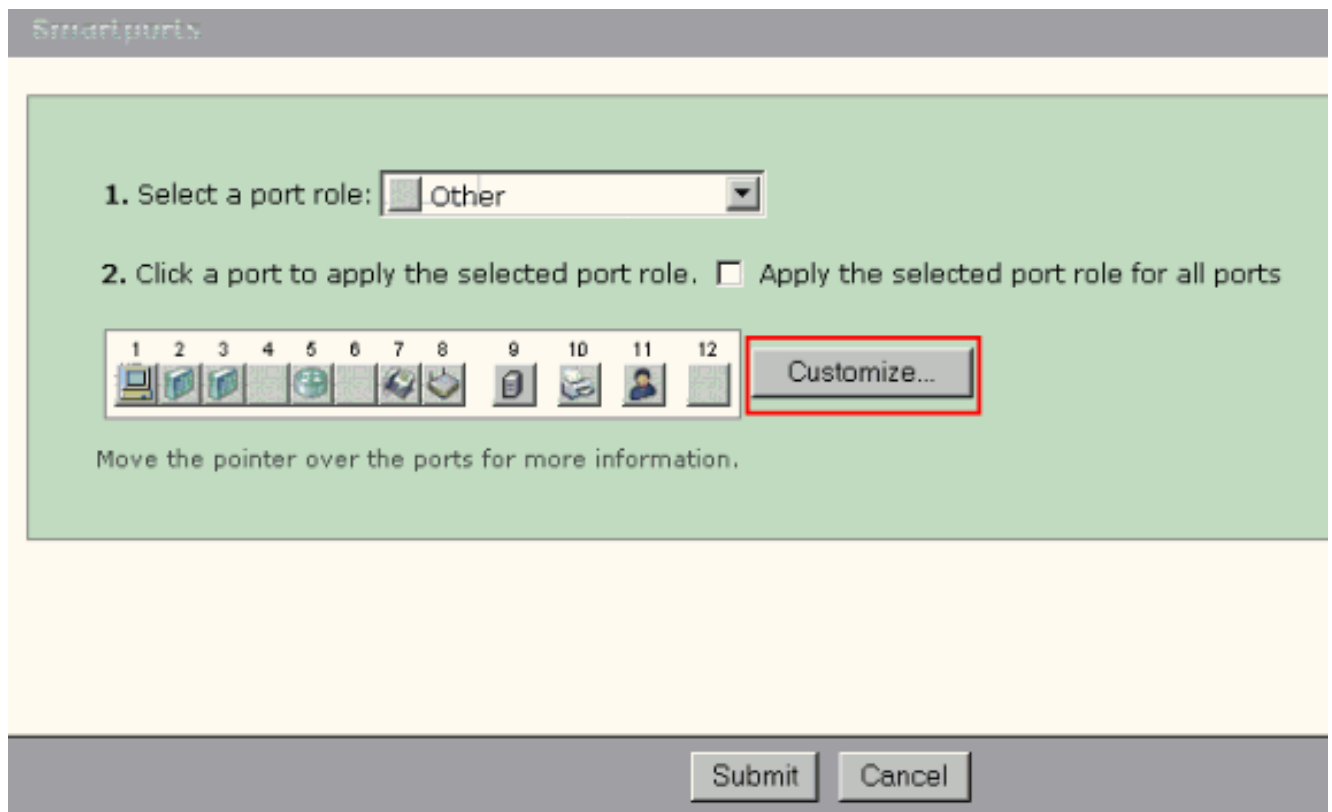
## [VLAN-lidmaatschap wijzigen](#)

Het specifieke VLAN-lidmaatschap kan worden gewijzigd voor de havens die deel uitmaken van deze Smartport-rollen:

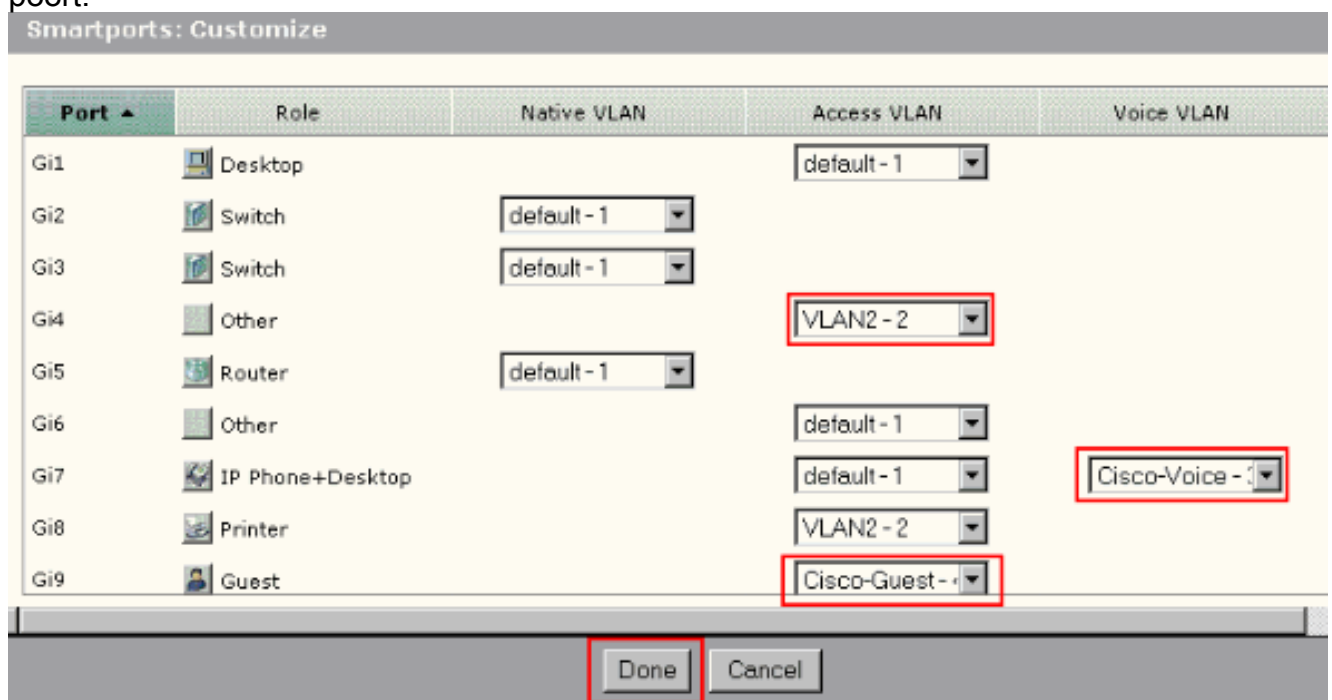
- **Native VLAN**-Switch, router en access point
- **Toegang tot VLAN**-desktop, IP-telefoon+desktop, server, printer, test en andere apparaten **Opmerking:** Toegang VLAN voor de rol van de Gast moet Cisco-Guest VLAN zijn.
- **Voice VLAN**-IP telefoon+Desktop Voice VLAN dient alleen het Cisco-Voice VLAN te zijn.

Gebruik het venster **Aanpassen** om poorten aan VLAN's toe te wijzen. Selecteer **Configureren > Smartports** in het menu Apparaatbeheer om dit venster weer te geven.

1. Klik op **Aanpassen** in het venster Smartports.



2. Kies geschikte VLAN's voor elke poort.



3. Klik op **Klaar**.
4. Klik op **Inzenden** om de wijzigingen op te slaan.

## [EtherChannel configureren](#)

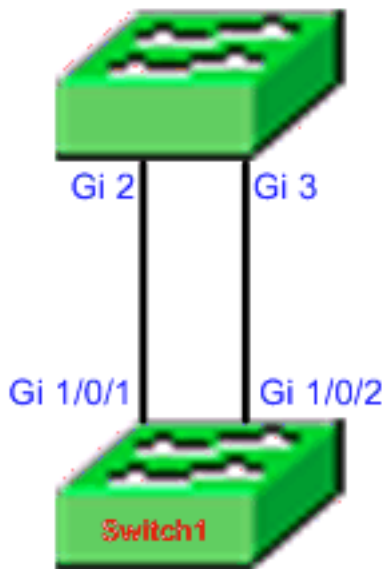
Een EtherChannel is een groep van twee of meer Fast Ethernet of Gigabit Ethernet switch poorten die in één logische link zijn gebundeld die een hogere bandbreedte tussen twee switches creëren. De switch ondersteunt maximaal zes EtherChannel-switches.

Alle havens in een EtherChannel moeten dezelfde kenmerken hebben:

- Alle havens zijn 10/100 of alle 10/100/1000 havens. U kunt een combinatie van 10/100 en 10/100/1000 poorten niet in een EtherChannel groeperen.
- Alle poorten hebben dezelfde snelheid en dubbele modus.
- Alle poorten worden toegepast met de Smartports Switch-poortrol en behoren tot hetzelfde VLAN.

Voltooi deze stappen om EtherChannel te maken tussen een Cisco Catalyst Express versie 500 en een andere switch:

### Cisco Catalyst Express CE500G-12TC Switch



### Cisco Catalyst 3750 Series Switch

1. Selecteer vanuit Apparaatbeheer van de Cisco Catalyst Express 500 switch **Configureren** > **EtherChannel** om het venster EtherChannel weer te geven.
2. Klik op **Maken**.
3. Voer de kanaalgroep-ID in.
4. Kies het Kanaalprotocol (modus) voor de lijst Modus. **Opmerking:** de Catalyst Express 500 switch ondersteunt twee modi, LACP en Static. Configureer de afstandsswitch in overeenstemming met de door u gekozen modus.
5. Klik op de selectietekens tegen de poorten die deel moeten uitmaken van het kanaal.
6. Klik op **Gereed** en klik op **Indienen** om de wijzigingen op te slaan.

EtherChannels: Create

Group [1-6]:

Mode:

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

7. Als u voor het LACP-protocol hebt gekozen om over het kanaal te onderhandelen, moet u de afstandsbediening configureren zoals deze uitvoer toont:

```
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
```

Als u ervoor kiest het kanaal statistisch te configureren, dient u de afstandsbediening te configureren zoals deze uitvoer toont:

```
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
```

## Verifiëren

Open het venster **Configure > EtherChannel** om de status van het gemaakte EtherChannel-venster te controleren. De status wordt weergegeven als 'In use'. Anders kunt u diagnostiek op de poorten uitvoeren om het probleem te bepalen.

EtherChannels		
Group	Ports	Status
1	Gi2, Gi3	In Use

Geef de opdracht voor samenvatting van het kanaal uit in de Cisco 3750-switch om de status van de EtherChannel-configuratie te controleren. Het veld Protocol in de uitvoer geeft LACP weer als het wordt gebruikt om over het kanaal te onderhandelen, blanco of anderszins.

```
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
```

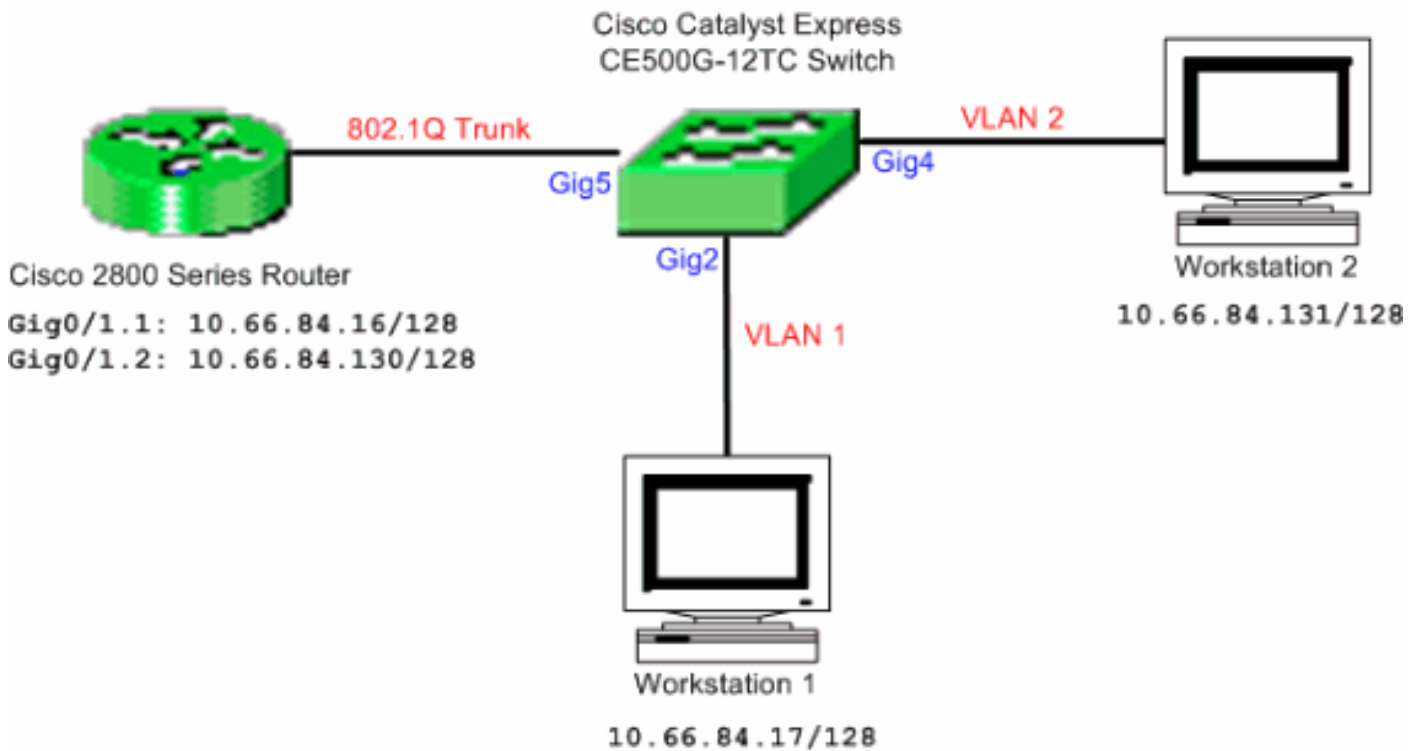
```
Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SU)        LACP      Gi1/0/1(P) Gi1/0/2(P)
```

U kunt het logbestand Catalyst 500 switch ook zien vanaf Monitor > Log in op apparaatbeheer. Dit voorbeeld toont de EtherChannel-foutmelding vanwege de verkeerde configuratie van EtherChannel op de afstandsswitch.

Alert Log		
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

## [InterVLAN-routing met een Cisco router](#)

### Netwerkdigram



**Opmerking:** de voorbeeldconfiguratie maakt gebruik van de Cisco 2800 Series router. Dit kan worden vervangen door een Cisco-router die IEEE 802.1Q trunking ondersteunt.

Voltooi deze stappen om de routing tussen VLAN's met een Cisco-router te configureren:

1. Volg deze stappen om de Cisco Catalyst Express 500 switch te configureren: Pas de rol van de Scheur van het Desktop op havens Gig2 en Gig4 toe. Zie de sectie van [Smartport op Havens](#) van dit document voor de configuratieprocedure toe passen. Pas de rol van de router Smartport toe op poort Gig5. Pas de juiste VLAN-id's op de poorten toe. Pas VLAN 1 aan als toegang VLAN voor de poort Gig2. Toewijzen VLAN 2 als toegang VLAN voor de poort Gig4. Pas VLAN 1 aan als het inheemse VLAN voor poort Gig5. Zie de sectie van [VLAN-Memberaties wijzigen](#) voor de configuratieprocedure.

2. Configureer de Cisco 2800 Series router:

```
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
```

## Verifiëren

Selecteer **Monitor > Port Status** op het apparaat Manager om de status van de switch poort op de Catalyst Express 500 switch te zien.

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

Controleer of de pingelen van werkstation 1 naar werkstation 2 passeert.

```
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
```

Start een overtrekken om het pad te controleren dat is genomen om te communiceren tussen Workstation 1 en Workstation 2.

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

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

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

```
Trace complete.
```

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

De Switched Port Analyzer (SPAN) optie, die soms port mirroring of port monitoring wordt genoemd, selecteert netwerkverkeer voor analyse door een netwerkanalyzer. De netwerkanalyzer kan een Cisco SwitchProbe-apparaat of een andere RMON-test (Remote Monitoring) zijn. De switch ondersteunt alleen de lokale SPAN en ondersteunt Remote SPAN niet.

De doelpoort moet worden geconfigureerd met de diagnostische rol in de zoekfunctie. Dit kan alleen worden gedaan met de Cisco Network Assistant-software. Raadpleeg [SPAN op Catalyst Express 500](#) voor het configureren van de Catalyst Express 500 switch om verkeer te bewaken.

## [Zet de Catalyst Express 500 Switch terug op fabrieksinstellingen](#)

Als u connectiviteit hebt met Apparaatbeheer van de switch en u de switch wilt terugstellen naar standaardinstellingen en de huidige Cisco IOS systeemsoftware wilt behouden, raadpleegt u de [Switch Reset met behulp van het](#) gedeelte [Apparaatbeheer](#) van [Reset Catalyst Express 500](#)

## [Series Switches naar standaardinstellingen.](#)

Als u geen connectiviteit hebt met Apparaatbeheer van de switch en u de switch wilt terugstellen naar de standaardinstelling van de fabriek, raadpleeg de [Reset de Switch wanneer Apparaatbeheer niet beschikbaar is](#) gedeelte van [Reset Catalyst Express 500 Series Switches naar standaardinstellingen van de fabriek](#).

Raadpleeg het gedeelte [Software voor Switch](#) van de [gebruikershandleiding voor Catalyst Express 500 Switches - Problemen oplossen](#) voor meer informatie over de herstelprocedure.

## [Verifiëren](#)

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

## [Problemen oplossen](#)

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## [Gerelateerde informatie](#)

- [Introductiegids voor de Catalyst Express 500 Switches](#)
- [Gebruikershandleiding voor Catalyst Express 500 Switches](#)
- [De betekenis van EtherChannel-taakverdeling en redundantie op Catalyst-Switches](#)
- [InterVLAN-routing en ISL/802.1Q trunking configureren op een Catalyst 2900XL/3500XL/2950 Switch met behulp van een externe router](#)
- [Productondersteuning voor switches](#)
- [Ondersteuning voor LAN-switching technologie](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)