Netwerken
Deel 2 – Switching, routing en draadloos

Netwerken
Deel 2 – Switching, routing en draadloos

Versie 7

John Bakker

Boom beroepsonderwijs · Meppel · 2021

Boom beroepsonderwijs
info@boomberoepsonderwijs.nl
www.boomberoepsonderwijs.nl

Auteur: John Bakker
Redactie en opmaak: Henk Pel, Zeist
Titel: Netwerken – Deel 2 – Switching, routing en draadloos
ISBN 978 90 372 5909 4
Eerste druk / eerste oplage

Inhoud

0 Switching, routing en draadloos

Welkom bij het tweede boek van het Cisco Networking Academy CCNAv7-curriculum, S*witching, routing en draadloos (SRWE)*. Dit is de tweede van drie boeken die op het CCNA-certificeringsexamen afgestemd zijn. Dit boek bevat 16 hoofdstukken met elk een reeks aan onderwerpen.

Switching, routing en draadloos vergroten je kennis van de werking van routers en switches in kleine netwerken. Het boek laat je kennismaken met draadloze lokale netwerken (WLAN's) en netwerkbeveiligingsconcepten.

Aan het einde van dit boek ben je in staat om geavanceerde functionaliteit in routers en switches te configureren. Je kunt ook eenvoudig troubleshooting voor deze componenten uitvoeren. Met behulp van best practices op het gebied van beveiliging zul je veelvoorkomende protocolproblemen in zowel IPv4- als IPv6-netwerken troubleshooten en oplossen.

De vaardigheden en kennis die je in dit boek opdoet, bereiden je voor op het laatste boek in CCNA. Met Cisco Networking Academy is er geen betere tijd dan nu. Aan de slag!

LET OP!

Om de Packet-Tracer- en Lab-activiteiten te kunnen uitvoeren heb je de nieuwste versie van Packet Tracer nodig. Hiervoor is een account bij de Cisco Networking Academy nodig.

Ga naar netacad.boomberoepsonderwijs.nl om je aan te melden via je **School-** of **Boom-account** en volg de stappen zoals deze vervolgens op de site aangegeven zijn.

Heb je nog geen account, registreer je dan eerst als gebruiker via **Registreer**.

1 Basisapparaatconfiguratie

1.0 Inleiding

1.0.1 Waarom zou je dit hoofdstuk bestuderen?

Welkom bij de basisapparaatconfiguratie!
Welkom bij het eerste hoofdstuk van CCNA *Switching, routing en draadloos*! Je weet dat switches en routers een ingebouwde configuratie hebben, dus waarom zou je moeten leren om switches en routers verder te configureren?

Stel dat je een modeltreinenset gekocht hebt. Nadat je de baan gelegd hebt, realiseer je je dat de rails slechts een eenvoudige ovale vorm hebben en dat de treinwagons alleen met de klok mee rijden. Misschien wil je dat de rails een acht vormen met een viaduct. Misschien wil je twee treinen hebben die onafhankelijk van elkaar werken en in verschillende richtingen rijden. Hoe kun je dat bereiken? Je moet het spoor en de bediening opnieuw configureren.

Hetzelfde geldt voor netwerkapparaten. Als netwerkbeheerder heb je gedetailleerde controle over de apparaten in je netwerk nodig. Dit betekent het configureren van de switches en routers zodat je netwerk doet wat je wilt. Dit hoofdstuk bevat meerdere Syntax-Checker- en Packet-Tracer-activiteiten om je te helpen deze vaardigheden te ontwikkelen. Laten we beginnen!

1.0.2 Wat leer je in dit hoofdstuk?

Er wordt uitgelegd hoe je apparaten met beveiligings-'best practices' configureert. De paragrafen in dit hoofdstuk zijn:

Onderwerp	Doel
Configureer een switch met de initiële instellingen	Configureer de initiële instellingen op een Cisco-switch
Switch-poorten configureren	Configureer de switch-poorten om aan de netwerkeisen te voldoen
Beveilig de externe toegang	Configureer de beveiligde beheertoegang voor een switch
Basisrouterconfiguratie	Configureer, met behulp van de CLI, de basisinstellingen op een router om tussen twee direct aangesloten netwerken te routeren
Verifieer directly connected netwerken	Controleer de connectiviteit tussen twee netwerken die direct met een router verbonden zijn

1.1 Configureer een switch met de initiële instellingen

1.1.1 Switch-boot-sequence

Voordat je een switch kunt configureren, moet je hem inschakelen en de vijf stappen van de opstartvolgorde laten doorlopen. Deze paragraaf behandelt de basisprincipes van het configureren van een switch en heeft aan het einde een Lab-activiteit.

Nadat een Cisco-switch ingeschakeld is, doorloopt hij de volgende vijf stappen:

1 Eerst laadt de switch een **POST**-programma (Power-ON Self Test) dat in **ROM** opgeslagen is. POST controleert het CPU-subsysteem. Het POST-programma test CPU, DRAM en het gedeelte van het flash-systeem waaruit het flash-bestandssysteem bestaat.

2 Vervolgens laadt de switch de boot-loader-software. De boot-loader is een klein programma dat in ROM opgeslagen is en onmiddellijk nadat de POST met succes voltooid is, uitgevoerd wordt.
3 De boot-loader voert een low-level CPU-initialisatie uit. De CPU-registers, die bepalen waar het fysieke geheugen toegewezen wordt, de hoeveelheid geheugen en de snelheid, worden geïnitialiseerd.
4 De boot-loader initialiseert het flash-bestandssysteem op het moederbord.
5 Tenslotte lokaliseert en laadt de boot-loader een standaard IOS-image in het geheugen en geeft de besturing van de switch over aan het IOS.

1.1.2 Het commando boot system

De switch probeert met behulp van de informatie in de **BOOT**-omgevingsvariabele automatisch op te starten. Als deze variabele niet ingesteld is, probeert de switch het eerste uitvoerbare bestand dat het kan vinden te laden en uit te voeren. Op Catalyst 2960-serie-switches bevindt het image-bestand zich normaal gesproken in een map met dezelfde naam als het imagebestand (met uitzondering van de .bin-bestandsextensie).

Het IOS-besturingssysteem initialiseert vervolgens met behulp van de IOS-commando's in het startup-config-bestand de interfaces. Het startup-config-bestand heet **config.text** en bevindt zich in flash.

In het voorbeeld wordt de **BOOT**-omgevingsvariabele met het globale configuratiecommando **boot system** ingesteld. Je ziet dat het IOS zich in een afzonderlijke map bevindt en dat het pad naar de map opgegeven is. Gebruik het commando **show boot** om te zien wat het huidige IOS-boot-bestand is.

```
S1(config)#
boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

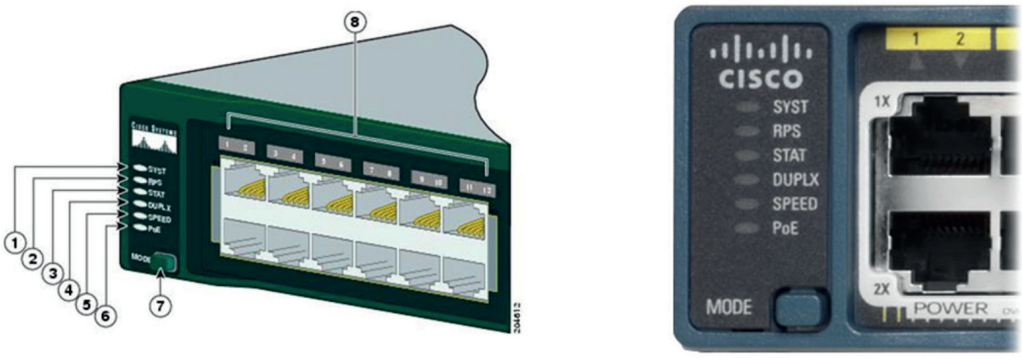
De tabel definieert elk deel van het **boot system**-commando.

Commando	Definitie
`boot system`	Het hoofdcommando
`flash:`	De locatie waar het bestand opgeslagen is
`c2960-lanbasek9-mz.150-2.SE/`	Het pad naar het bestandsysteem
`c2960-lanbasek9-mz.150-2.SE.bin`	De IOS-bestandsnaam

1.1.3 Switch-LED-indicatoren

Cisco Catalyst-switches hebben verschillende status-LED's. Je kunt de switch-LED's gebruiken om de activiteit en prestaties van de switch snel te controleren. Switches van de verschillende modellen en functiesets hebben verschillende LED's en de plaatsing op het frontpaneel van de switch kan eveneens variëren.

In figuur 1-1 zijn de switch-LED's en de mode-knop van de Cisco Catalyst 2960-switch te zien.



Figuur 1-1 *Indicatie-LED's van de Catalyst 2960-switch*

De mode-knop (7 in figuur 1-1) wordt gebruikt om tussen poortstatus, poortduplex, poortsnelheid en, als dat ondersteund wordt, de **Power over Ethernet** (PoE)-status van de poort-LED's (8 in de figuur) te schakelen.

Hieronder staat het doel van de LED's (1 t/m 6 in figuur 1-1) en de betekenis van de kleuren.

System-LED (1)

Geeft aan dat het systeem spanning heeft en naar behoren functioneert. Als de LED uit is, betekent dit dat het systeem niet ingeschakeld is. Als de LED groen is, werkt het systeem normaal. Als de LED oranje is, heeft het systeem spanning maar werkt het niet goed.

Redundant Power System (RPS) LED (2)

Geeft de RPS-status weer. Als de LED uit is, is het RPS uit of is dit niet correct aangesloten. Als de LED groen is, is het RPS aangesloten en gereed om back-up-voeding te leveren. Als de LED groen knippert, is het RPS aangesloten maar niet beschikbaar omdat dit een ander apparaat van spanning voorziet. Als de LED oranje is, bevindt het RPS zich in de standby-mode of heeft het een storing. Als de LED oranje knippert, is de interne voeding van de switch defect en levert het RPS de spanning.

Poortstatus-LED (3)

Geeft aan dat de poortstatus geselecteerd is wanneer de LED groen is. Dit is de standaard mode. Als deze mode geselecteerd is, geven de poort-LED's kleuren met verschillende betekenissen weer. Als de poort-LED uit is, is er geen verbinding of is de poort administratief uitgeschakeld (**shutdown**). Als de poort-LED groen is, is er een verbinding aanwezig. Als de poort-LED groen knippert, is er een activiteit en verstuurt of ontvangt de poort data. Als de poort-LED groen/oranje wisselt, is er een verbindingsfout. Als de poort-LED oranje is, is de poort geblokkeerd om ervoor te zorgen dat er geen loop ontstaat in het forwarding-domein en stuurt het geen data door (poorten blijven meestal de eerste 30 seconden na activering in deze status). Als de poort-LED oranje knippert, is de poort geblokkeerd om een mogelijke loop in het forwarding-domein te voorkomen.

Poort-duplex-LED (4)

Geeft aan dat de poort-duplex-mode geselecteerd is wanneer de LED groen is. Als deze mode geselecteerd is, bevinden de poorten waarvan de poort-LED's uit zijn zich in half-duplex-mode. Als de poort-LED groen is, bevindt de poort zich in full-duplex-mode.

Poortsnelheid-LED (5)

Geeft aan dat de poortsnelheids-mode geselecteerd is. Als deze mode geselecteerd is, geven de poort-LED's kleuren met verschillende betekenissen weer. Als de poort-LED uit is, werkt de poort op 10 Mb/s. Als de poort-LED groen is, werkt de poort op 100 Mb/s. Als de LED groen knippert, werkt de poort op 1000 Mb/s.

Power over Ethernet (PoE) mode LED (6)

Als PoE ondersteund wordt, is een PoE-mode-LED aanwezig. Als de LED uit is, geeft dit aan dat de PoE-mode niet geselecteerd is en dat geen van de poorten spanning geweigerd is of in storing staat. Als de LED oranje knippert, is de PoE-mode niet geselecteerd, maar is aan ten minste één poort spanning geweigerd of is een poort in storing. Als de PoE-LED groen is, geeft dit aan dat de PoE-mode geselecteerd is en geven de poort-LED's kleuren met verschillende betekenis weer. Als de poort-LED uit is, is de PoE uit. Als de poort-LED groen is, is de PoE aan. Als de poort-LED groen/oranje afwisselt, wordt PoE geweigerd omdat de stroomvoorziening van de switch door het gevoede apparaat te zwaar belast wordt. Als de poort-LED oranje knippert, is de PoE vanwege een fout uitgeschakeld. Als de poort-LED oranje is, is PoE voor de poort uitgeschakeld.

1.1.4 Herstellen van een systeemcrash

De boot-loader biedt toegang tot de switch als het besturingssysteem vanwege ontbrekende of beschadigde systeembestanden niet gebruikt kan worden. De boot-loader heeft een command-line die toegang tot de bestanden geeft die in het flashgeheugen opgeslagen zijn.

De boot-loader is via een consoleverbinding toegankelijk door de volgende stappen te volgen:

1. Sluit een PC met een consolekabel op de switch-console-poort aan. Configureer de terminal-emulatiesoftware om verbinding met de switch te maken.
2. Koppel het netsnoer van de switch af.
3. Sluit het netsnoer van de switch weer aan en druk binnen 15 seconden op de mode-knop en houd deze ingedrukt terwijl de systeem-LED nog groen knippert.
4. Houd de mode-knop ingedrukt totdat de systeem-LED kort oranje en vervolgens ononderbroken groen wordt. Laat vervolgens de mode-knop los.
5. De boot-loader-prompt **switch:** verschijnt in de terminal-emulatiesoftware op de switch.

Typ **help** of **?** op de boot-loader-prompt om een overzicht van de beschikbare commando's te bekijken.

De switch probeert standaard automatisch met behulp van de informatie in de **BOOT**-omgevingsvariabele op te starten.

```
switch: set
BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin
(output omitted)
switch: flash_init
Initializing Flash...
flashfs[0]: 2 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11838464
flashfs[0]: Bytes available: 20675584
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.
```

Nadat flash geïnitialiseerd is, kun je het commando **dir flash:** invoeren om de mappen en bestanden in flash te bekijken, zoals hieronder te zien is.

```
switch: dir flash:
Directory of flash:/
    2  -rwx  11834846                c2960-lanbasek9-mz.150-2.SE8.bin
    3  -rwx  2072                    multiple-fs
```

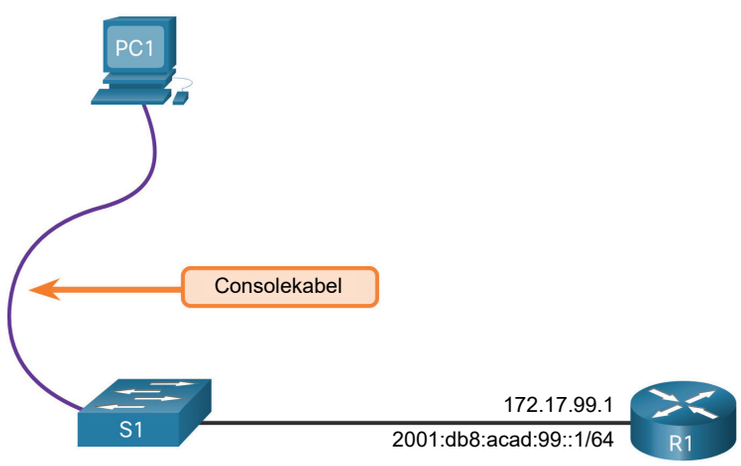
Voer het commando **BOOT=flash** in om het pad van de **BOOT**-omgevingsvariabele te wijzigen dat de switch gebruikt om het nieuwe IOS in flash te laden. Voer opnieuw het commando **set** in om het nieuwe pad van de **BOOT**-omgevingsvariabele te verifiëren. Tenslotte typ je het **boot**-commando zonder argumenten in om het nieuwe IOS te laden, zoals hieronder te zien is.

```
switch: BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
switch: set
BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
(output omitted)
switch: boot
```

De boot-loader-commando's ondersteunen het initialiseren van flash, het installeren van een nieuw IOS, het wijzigen van de BOOT-omgevingsvariabele en het herstel van verloren of vergeten wachtwoorden.

1.1.5 Toegang tot het switch-beheer

Om een switch op remote beheer voor te bereiden, moet de switch met een IP-adres en een subnetmasker geconfigureerd worden. Houd er rekening mee dat op de switch een default gateway geconfigureerd moet worden om de switch vanaf een extern netwerk te kunnen beheren. Dit lijkt erg op het configureren van de IP-adresinformatie voor host-apparaten. In figuur 1-2 moet aan de **Switch Virtual Interface** (SVI) van S1 een IP-adres toegewezen worden. De SVI is een virtuele interface, geen fysieke poort op de switch. Een consolekabel wordt gebruikt om verbinding met een PC te maken, zodat de switch geconfigureerd kan worden.



Figuur 1-2 *PC-aansluiting om de switch te configureren*

1.1.6 Voorbeeld voor het configureren van de SVI van een switch

Standaard is de switch zo geconfigureerd dat het beheer ervan via VLAN 1 gecontroleerd wordt. Alle poorten zijn standaard aan VLAN 1 toegewezen. Om veiligheidsredenen wordt het als **best practice** gezien om een ander VLAN dan VLAN 1 te gebruiken voor het beheer-VLAN, zoals VLAN 99 in het voorbeeld.

De stappen voor het configureren van de toegang voor het switch-beheer zijn:

Configureer de beheerinterface

In de VLAN-interfaceconfiguratie-mode wordt een IPv4-adres en subnetmasker aan de beheer-SVI van de switch toegewezen.

Opmerking De SVI van VLAN 99 verschijnt niet 'up/up' totdat VLAN 99 aangemaakt is en er een apparaat op een switch-poort aangesloten is dat aan VLAN 99 gekoppeld is.

Opmerking De switch moet misschien ook voor IPv6 geconfigureerd worden. Voordat je een IPv6-adres op bijvoorbeeld een Catalyst 2960-switch met IOS-versie 15.0 kunt configureren, moet je het globale configuratiecommando **sdm prefer dual-ipv4-and-ipv6 default** invoeren en de switch opnieuw opstarten (reload).

IOS-commando's	Taak
S1# **configure terminal**	Ga naar de globale configuratie-mode.
S1(config)# **interface vlan 99**	Ga naar de interfaceconfiguratie-mode voor de SVI.
S1(config-if)# **ip address 172.17.99.11 255.255.255.0**	Configureer het beheer-interface-IPv4-adres.
S1(config-if)# **ipv6 address 2001:db8:acad:99::1/64**	Configureer het beheer-interface-IPv6-adres.
S1(config-if)# **no shutdown**	Activeer de beheer-interface.
S1(config-if)# **end**	Ga naar de privileged-EXEC-mode.
S1# **copy running-config startup-config**	Bewaar de running-config in de startup-config.

Configureer de default gateway

De switch moet met een default gateway geconfigureerd worden als deze op afstand vanuit netwerken beheerd wordt, die niet direct verbonden zijn.

Opmerking Omdat de default gateway-informatie van een Router-Advertisement-bericht (RA-bericht) ontvangen wordt, heeft de switch geen IPv6-default gateway nodig.

IOS-commando's	Taak
S1# **configure terminal**	Ga naar de globale configuratie-mode.
S1(config)# **ip default-gateway 172.17.99.1**	Configureer de default gateway voor de switch.
S1(config-if)# **end**	Ga naar de privileged-EXEC-mode.
S1# **copy running-config startup-config**	Bewaar de running-config in de startup-config.

Verifieer de connectiviteit

De commando's **show ip interface brief** en **show ipv6 interface brief** zijn handig om de status van zowel de fysieke als virtuele interfaces te bepalen. De onderstaande uitvoer bevestigt dat de interface VLAN 99 met een IPv4- en IPv6-adres geconfigureerd is.

Opmerking Een IP-adres dat op de SVI toegepast wordt, is alleen voor externe toegang tot de switch, hiermee kan de switch geen laag-3-packets routeren.

```
S1# show ip interface brief
Interface     IP-Address     OK? Method   Status    Protocol
Vlan99        172.17.99.11   YES manual   down      down
(output omitted)
S1# show ipv6 interface brief
Vlan99                 [down/down]
    FE80::C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99::1
(output omitted)
```

1.1.7 Lab – Basis switch-configuratie

In dit Lab voer je de volgende opdrachten uit:

- Sluit het netwerk aan en controleer de default configuratie van de switch.
- Configureer de basisinstellingen van het netwerkapparaat.
- Controleer en test de connectiviteit.
- Beheer de MAC-adrestabel.

Download de opdracht in pdf-formaat in de NetAcad-omgeving.

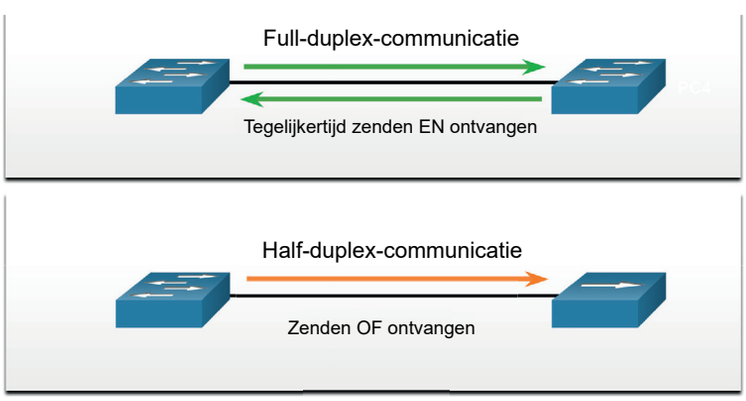
1.2 Configureer de switch-poorten

1.2.1 Duplex-communicatie

De poorten van de switch kunnen onafhankelijk van elkaar voor verschillende behoeften geconfigureerd worden. In deze paragraaf wordt uitgelegd hoe je switch-poorten configureert, hoe je de configuraties verifieert, welke fouten veel voorkomen en hoe je problemen met switch-configuraties troubleshoot.

Full-duplex-communicatie verhoogt de efficiëntie van de bandbreedte doordat beide uiteinden van een verbinding tegelijkertijd data kunnen verzenden en ontvangen. Dit wordt bidirectionele communicatie genoemd en vereist microsegmentatie. Een micro-gesegmenteerd LAN ontstaat wanneer er slechts één apparaat op een switch-poort aangesloten is en in full-duplex-mode werkt. Er is geen collision-domein geassocieerd met een switch-poort die in full-duplex-mode werkt.

In tegenstelling tot full-duplex-communicatie is half-duplex-communicatie unidirectioneel. Half-duplex-communicatie veroorzaakt prestatieproblemen omdat data slechts in één richting tegelijk kunnen stromen, wat vaak tot collisions (botsingen) leidt. Half-duplex-verbindingen zijn meestal te vinden bij oudere hardware, zoals hubs. Full-duplex-communicatie heeft bij de meeste hardware half-duplex vervangen.

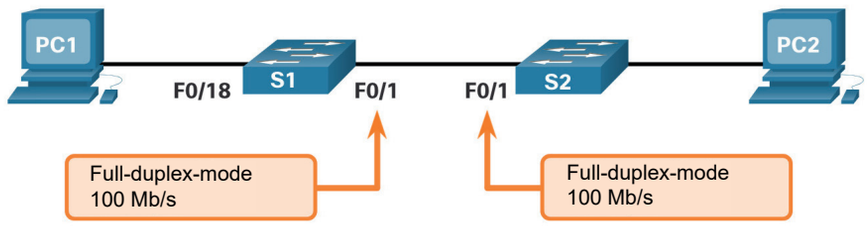


Figuur 1-3 *Verschil tussen full- en half-duplex*

GigabitEthernet en 10 Gb NIC's vereisen full-duplexverbindingen om te kunnen functioneren. In full-duplex-mode is het collision-circuit van de NIC uitgeschakeld. Full-duplex biedt 100 procent efficiëntie in beide richtingen (verzenden en ontvangen). Dit resulteert in een verdubbeling van het potentiële gebruik van de opgegeven bandbreedte.

1.2.2 Configureer switch-poorten op de fysieke laag

Switch-poorten kunnen handmatig met specifieke duplex- en snelheidsinstellingen geconfigureerd worden. Gebruik het interfaceconfiguratiecommando **duplex** om de duplex-mode voor een switch-poort handmatig op te geven. Gebruik het interfaceconfiguratiecommando **speed** om de snelheid handmatig op te geven. Beide switches in de topologie moeten bijvoorbeeld altijd in full-duplex met 100 Mb/s functioneren.



Figuur 1-4 *Switch-poort-instellingen moeten aan beide zijden gelijk zijn*

De tabel geeft de commando's voor S1. Dezelfde commando's kunnen op S2 toegepast worden.

IOS-commando's	Taak
S1# `configure terminal`	Ga naar de globale configuratie-mode.
S1(config)# `interface FastEthernet 0/1`	Ga naar de interfaceconfiguratie-mode.
S1(config-if)# `duplex full`	Configureer de interface-duplex.
S1(config-if)# `speed 100`	Configureer de interfacesnelheid.
S1(config-if)# `end`	Ga naar de privileged-EXEC-mode.
S1# `copy running-config startup-config`	Bewaar de running-config in de startup-config.

De standaardinstelling voor zowel duplex als snelheid voor switch-poorten op Catalyst 2960- en 3560-switches is **auto**. De 10/100/1000-poorten werken in half- of full-duplex-mode wanneer ze ingesteld zijn op 10 of 100 Mb/s en werken alleen in full-duplex-mode wanneer ze op 1000 Mb/s (1 Gb/s) ingesteld zijn. Autonegotiation is handig wanneer de snelheid en duplexinstellingen van het apparaat dat met de poort verbinding maakt onbekend zijn of kunnen veranderen. Als je verbinding met bekende apparaten maakt, zoals servers, speciale werkstation of netwerkapparaten, is het een goed idee om de instellingen voor snelheid en duplex handmatig in te stellen.

Bij het troubleshooten van switch-poortproblemen is het belangrijk dat de instellingen voor duplex en snelheid gecontroleerd worden.

Opmerking Niet-overeenkomende instellingen voor duplex-mode en snelheid van switch-poorten kunnen verbindingsproblemen veroorzaken. Autonegotiation-storingen zorgen voor niet-overeenkomende instellingen.

Alle glasvezelpoorten, zoals 1000BASE-SX-poorten, werken alleen met één vooraf ingestelde snelheid en zijn altijd full-duplex.

1.2.3 Auto-MDX

Tot voor kort waren bepaalde kabeltypen (straight-through of crossover) nodig voor het aansluiten van apparaten. Switch-to-switch- en switch-to-router-verbindingen hadden verschillende Ethernet-kabels nodig. Het gebruik van **Automatic Medium-Dependent Interface crossover** (auto-MDIX) op een interface lost dit probleem op. Wanneer auto-MDIX ingeschakeld is, detecteert de interface automatisch het vereiste type kabelverbinding (straight-through of crossover) en configureert de verbinding op de juiste wijze. Wanneer je een verbinding met switches zonder auto-MDIX-functie maakt, moeten straight-through-kabels gebruikt worden om verbinding met apparaten zoals servers, werkstations of routers te maken. Crossover-kabels moeten gebruikt worden om verbinding met andere switches of repeaters te maken.