Probleemoplossing voor MAC-flaps/Loop op Cisco Catalyst-Switches

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met de MAC Flaps/Loop op Cisco Catalyst Switches.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van basisswitchingconcepten en inzicht in Spanning Tree Protocol (STP) en zijn functies op Cisco Catalyst-Switches.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst-Switches met alle versies (dit

document is niet beperkt tot enige specifieke software- of hardwareversies).

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document dient als een handleiding voor een systematische benadering van probleemoplossing met MAC-flaps of -problemen op de Cisco Catalyst-switches. MAC flaps/loops zijn verstoringen in een netwerk veroorzaakt door inconsistenties in de MAC-adrestabellen van switches. Dit document bevat niet alleen stappen om deze kwesties te identificeren en op te lossen, maar ook praktische voorbeelden voor een beter begrip.

Wat is MAC Flapping?

Een MAC-flap treedt op wanneer een switch een frame ontvangt met hetzelfde MAC-bronadres maar van een andere interface dan de interface waarvan hij het eerst leerde. Dit zorgt ervoor dat de switch tussen de poorten knippert en de MAC-adrestabel bijwerkt met de nieuwe interface. Deze situatie kan instabiliteit in het netwerk veroorzaken en tot prestatiekwesties leiden.

In een Cisco-switch wordt MAC-flapping meestal als een bericht zoals dit vastgelegd:

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

In dit voorbeeld werd het MAC-adres`xxxx.xxxx.xxxx`eerst geleerd op interfacepoort (1) en vervolgens op interfacepoort (2), waardoor een MAC-flap ontstond.

De meest voorkomende oorzaak van MAC-flapping is een Layer 2-lus in het netwerk, vaak als gevolg van een verkeerde configuratie van STP of problemen met redundante koppelingen. Andere oorzaken kunnen defecte hardware, software bugs, of zelfs security problemen zoals MAC spoofing.

Het oplossen van problemen met MAC-flaps impliceert vaak het identificeren en oplossen van alle loops in het netwerk, het controleren van apparaatconfiguraties, of het bijwerken van apparaatfirmware/software.

Algemene richtlijnen voor troubleshooting

- Identificeer de MAC-flapping: zoek naar logbestanden in uw switch die MAC-flapping aangeven. In een Cisco-switch ziet het logbericht er bijvoorbeeld als volgt uit:

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- Let op het MAC-adres en de interfaces: het logboekbericht geeft u het MAC-adres dat flapt en de interfaces waar het tussen flapt. Neem hier nota van omdat ze helpen bij uw onderzoek.
- Onderzoeken van de betrokken interfaces: gebruik de CLI van de switch om de betrokken interfaces te onderzoeken. U kunt opdrachten zoals`show interfaces`of`show mac address-table`gebruiken om te zien welke apparaten zijn aangesloten op de interfaces en waar het MAC-adres wordt geleerd.
- Overtrekken van het Flapping MAC-adres: MAC leert door poorten X en Y. Een poort leidt ons naar waar die MAC is aangesloten en de andere leidt ons naar de lus. Kies een poort en begin te werken met`show mac address-table`opdracht op elke Layer 2-switch in het pad.
- Controle voor fysieke Lussen: Kijk naar uw netwerktopologie om te zien of er fysieke lussen zijn. Deze kunnen voorkomen als er meerdere paden tussen de switches bestaan. Als een lijn wordt gevonden, moet u uw netwerk aanpassen om de lijn te verwijderen.
- Controleer STP: STP is ontworpen om lusjes in uw netwerk te voorkomen door bepaalde paden te blokkeren. Als STP verkeerd wordt geconfigureerd, voorkomt het geen lusjes zoals het moet zijn. Gebruik opdrachten zoals`show spanning-tree`om de STP-configuratie te controleren. Controleer ook of u topologische wijzigingsmeldingen (TCN's) gebruikt in de opdracht`show spanning-tree detail | include ieee|occur|from|is`.
- Controleer op dubbele MAC-adressen: als twee apparaten op uw netwerk hetzelfde MAC-adres hebben (meestal te zien in High Availability (HA)-instellingen en meerdere Network Interface Controller of Cards (NIC's)), kan dit MAC-flappen veroorzaken. Gebruik de opdracht`show mac address-table`om dubbele MAC-adressen op uw netwerk te zoeken.
- Controleren op defecte hardware of kabels: defecte netwerkkabels of hardware kunnen ervoor zorgen dat frames worden verzonden naar de verkeerde interfaces, wat kan leiden tot MAC flapping. Controleer de fysieke conditie van uw kabels en overweeg het uitwisselen van hardware om te zien of het probleem blijft bestaan. Het flappen van de interface kan ook het flappen van MAC op switches veroorzaken.
- Controleer op softwarebugs: soms kan MAC-flapping worden veroorzaakt door bugs in de software van uw netwerkapparaten. Controleer de Bug zoekfunctie.

Zoekfunctie voor bugs: https://bst.cloudapps.cisco.com/bugsearch

Help bij bugzoekfunctie:
https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

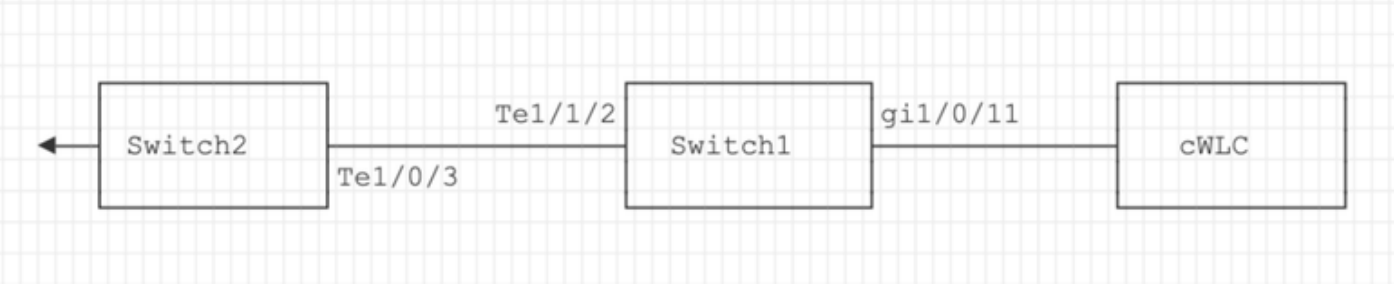
- Contact opnemen met TAC-ondersteuning: als u alles hebt geprobeerd en het probleem blijft bestaan, kan het tijd worden om contact op te nemen met Cisco TAC-ondersteuning. Zij kunnen verdere hulp bieden.

Casestudy 1

Probleembeschrijving

De eWLC-controller ondervindt een verlies aan connectiviteit met de gateway en pakketdruppels voorkomen dat AP's zich bij de controller aansluiten.

Topologie



Stappen voor probleemoplossing

MAC-flapping is geïdentificeerd op de switch (Switch 1) die is aangesloten op de eWLC.

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

MAC Learning:

Voer de opdrachtshow mac address-table address
in om het op de poort aangeleerde MAC-adres te controleren.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    DYNAMIC     Gi1/0/11


   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

Configuratie van poorten Gi1/0/11 en Te1/1/2:

Voer de opdrachtshow running-config interface
in om de interfaceconfiguratie te controleren.

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

CDP Buren van poorten Gi1/0/11 en Te1/1/2:

Voer de opdrachtshow cdp neighbors
in om de gegevens van de aangesloten apparaten te controleren.

<#root>

```
Switch1#show cdp neighbors gi1/0/11


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller



Switch1#show cdp neighbors gi1/1/2


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Switch2


                Ten 1/1/2         163            R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

MAC Learning on Switch 2 (uplink Switch):

Voer de opdrachtshow mac address-table address
in om het op de poort aangeleerde MAC-adres te controleren.

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC

Vl4 < ----- VRRP MAC of Vlan4


   4    0000.5e00.0101    DYNAMIC

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)
```

<#root>

```
Switch2#show vrrp  vlan 4


Vlan4 - Group 1

 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x

  Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4


  Advertisement interval is 1000 msec
```

Hoofdoorzaak

Er werd gecontroleerd dat de Virtual Router Redundancy Protocol (VRRP) ID van Switch 2 en de eWLC hetzelfde waren, wat resulteerde in het genereren van dezelfde Virtual MAC door de VRRP.

Resolutie

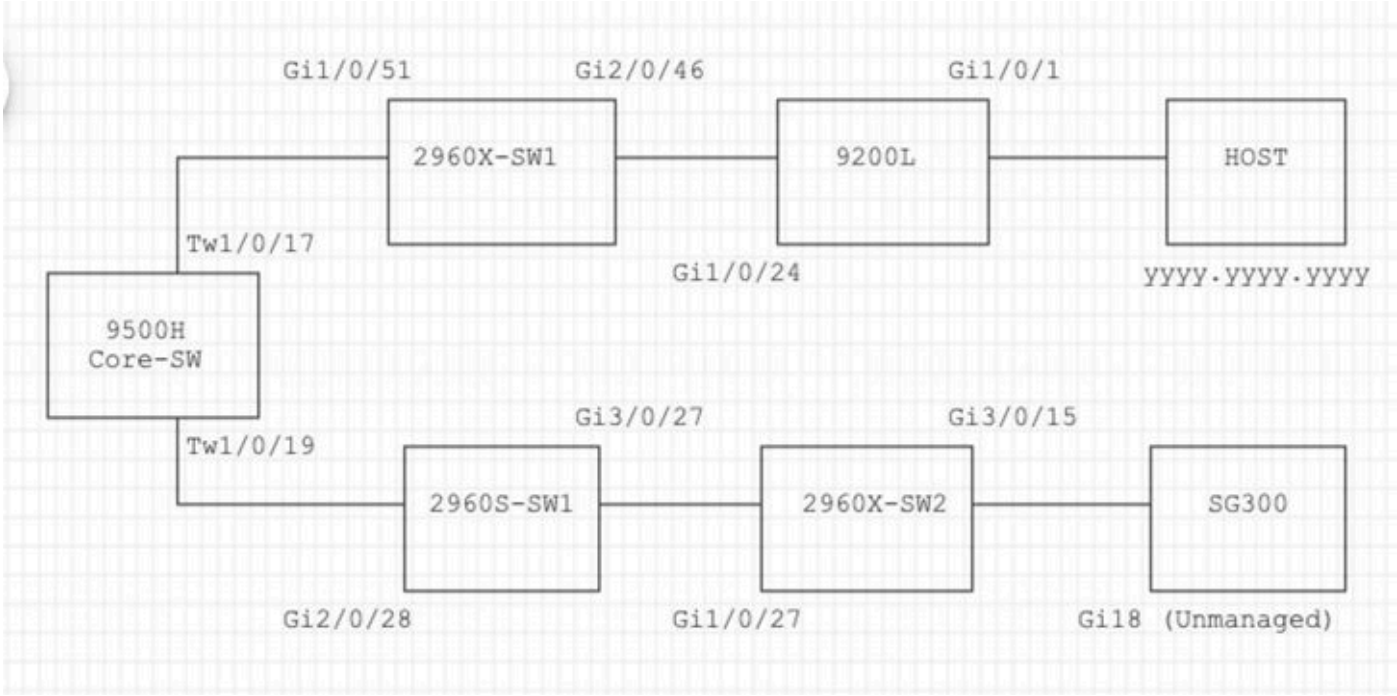
De kwestie werd opgelost na het veranderen van de VRRP instantie op de WLC, die een dubbele MAC op de switch veroorzaakte die tot een verlies van connectiviteit aan de gateway en pakketdalingen leidde, die APs verhinderden zich bij het controlemechanisme aan te sluiten.

Casestudy 2

Probleembeschrijving

Sommige servers zijn ontoegankelijk of hebben te maken met een aanzienlijke latentie/daling.

Topologie



Stappen voor probleemoplossing

1. Merkbare MAC flapping op de Core switch.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. Kies het MAC-adres`yyyy.yyyy.yyyy`voor het probleemoplossingsproces.

MAC Learning:

Voer de opdracht`show mac address-table address`
in om het op de poort aangeleerde MAC-adres te controleren.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

CDP Buren van poorten Twe 1/0/17 en Twe 1/0/17:

Voer de opdrachtshow cdp neighbors
in om de gegevens van de aangesloten apparaten te controleren.

<#root>

```
Core-SW#show cdp neighbors Twe 1/0/17


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960X-SW1

                 Twe 1/0/17        162              S I   WS-C2960X Gig 1/0/51



Core-SW#show cdp neighbors Twe 1/0/19


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960S-SW1

                 Twe 1/0/19        120              S I   WS-C2960S Gig 2/0/28
```

Logbestanden vanaf 2960X-SW1 aangesloten op Core-SW Twe1/0/17:

MACyyyy.yyyy.yyyyflapt tussen poort Gi1/0/51 en Gi2/0/46 (9200L).

<#root>

```
2960X-SW1#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51
```

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

2960X-SW1#show run interface gi 1/0/51

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

2960X-SW1#show run interface gi 2/0/46

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

Logbestanden vanaf 9200L:

(Dit lijkt de geldige poort te zijn voor dit MAC-adres.)

<#root>

9200L#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

9200L#show run interface gi 1/0/1

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

2960S-SW1 aangesloten op Core-SW Twe1/0/19:

(Dit is een pad voor een lus.) De haven op de Core-SW werd gesloten om de lus te verzachten.

Echter, MAC-flaps werden nog steeds waargenomen op de Core-SW.

Logbestanden vanaf 2960S-SW1:

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

2960S-SW1#show run interface gi 3/0/27

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

2960S-SW1#show cdp neighbor gi 3/0/27

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW2

Gig 3/0/27 176 S I WS-C2960X Gig 1/0/27

Logbestanden vanaf 2960X-SW2:

<#root>

```
2960X-SW2#show run interface gi 3/0/15


Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end


2960X-SW2#show cdp neighbor gi 3/0/15


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

SG300     Gig 3/0/15        157              S I   SG300-28P gi18




2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

Hoofdoorzaak

MAC-flaps werden gezien door de SG300 (onbeheerde) switch die was aangesloten op het netwerk.

Resolutie

Het probleem van de MAC-flapping werd opgelost door de poort te sluiten die was aangesloten op de onbeheerde switch SG300.

Preventie

STP Portfast:

STP PortFast zorgt ervoor dat een Layer 2 LAN-poort de doorsturen staat onmiddellijk ingaat, waarbij de luisterstatus en de leerstatus worden omzeild. STP PortFast voorkomt de generatie van STP-TCP's, die niet betekenisvol zijn vanaf poorten die geen STP Bridge Protocol Data Units (BPDU's) ontvangen. Configureer STP PortFast alleen op poorten die zijn verbonden met eindhostapparaten die VLAN's beëindigen en van waaruit de poort nooit STP BPDU's moet

ontvangen, zoals werkstations, servers en poorten op routers die niet zijn geconfigureerd om overbrugging te ondersteunen.

BPDU Guard:

STP BPDU Guard vult de functionaliteit van STP PortFast aan. Op STP-poorten die Fast-enabled zijn, beschermt STP BPDU Guard Layer 2-lijnen die STP niet kan leveren wanneer STP PortFast is ingeschakeld. STP BPDU Guard sluit poorten af die BPDU's ontvangen.

Root Guard:

Root guard voorkomt dat poorten STP root poorten worden. Gebruik STP Root Guard om te voorkomen dat ongeschikte poorten STP root poorten worden. Een voorbeeld van een ongeschikte poort is een poort die koppelt naar een apparaat dat buiten de directe administratieve controle van het netwerk valt.

Loop Guard:

Loop guard is een eigen optimalisatie van Cisco voor de STP. Loop guard beschermt Layer 2-netwerken tegen lussen die optreden wanneer iets de normale doorsturen van BPDU's op point-to-point links verhindert (bijvoorbeeld een storing in de netwerkinterface of een bezette CPU). Loop guard vult de bescherming tegen unidirectionele link failures aan die wordt geboden door Unidirectional Link Detection (UDLD). Loop guard isoleert storingen en laat STP convergeren naar een stabiele topologie waarbij de mislukte component wordt uitgesloten van de STP topologie.

BPDU-filter:

Dit schakelt de STP uit. BPDU's worden na ontvangst niet verzonden of verwerkt. Het is gemeenschappelijk met dienstverleners, niet noodzakelijk ondernemingsnetwerken.

UDLD:

Het Cisco-bedrijfseigen UDLD-protocol bewaakt de fysieke configuratie van de koppelingen tussen apparaten en poorten die UDLD ondersteunen. UDLD detecteert het bestaan van unidirectionele links. UDLD kan zowel in de normale als in de agressieve modus werken. Normal-mode UDLD classificeert een link als unidirectioneel als de ontvangen UDLD-pakketten geen informatie bevatten die correct is voor het buurapparaat. Naast de functionaliteit van de normale modus UDLD, brengt de agressieve modus UDLD poorten in de fout-uitgeschakelde toestand als de relatie tussen twee eerder gesynchroniseerde buren niet kan worden hersteld.

Stormcontrole:

Traffic storm control is geïmplementeerd in hardware en heeft geen invloed op de algehele prestaties van de switch. Eindstations, zoals pc’s en servers, zijn doorgaans de bron van uitzendverkeer dat kan worden onderdrukt. Om onnodige verwerking van overtollig uitzendingsverkeer te vermijden, laat de controle van het verkeersonweer voor uitzendingsverkeer op toegangspoorten toe die met eindstations en op poorten verbinden die met zeer belangrijke netwerkknooppunten verbinden.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.