DHCP Snooping voor Packets Crossing Layer 3 Hops begrijpen

Inhoud

Inleiding

Dit document beschrijft de interacties en het gedrag van DHCP-snuffelaars wanneer het pakket een L3-apparaat kruist en als het pakket is ingekapseld in L3-header.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS® XE-vaardigheid in configuratie en operationele opdrachten.
- De Cisco Catalyst 9000-serie switch hardware en architectuur.
- Een goed begrip van DHCP-protocolbewerkingen en DHCP-snuffelmechanismen.
- Een conceptueel begrip van DHCP optie 82 en de rol van de relay agent.
- Basiskennis van routeringsprotocollen.

Gebruikte componenten

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

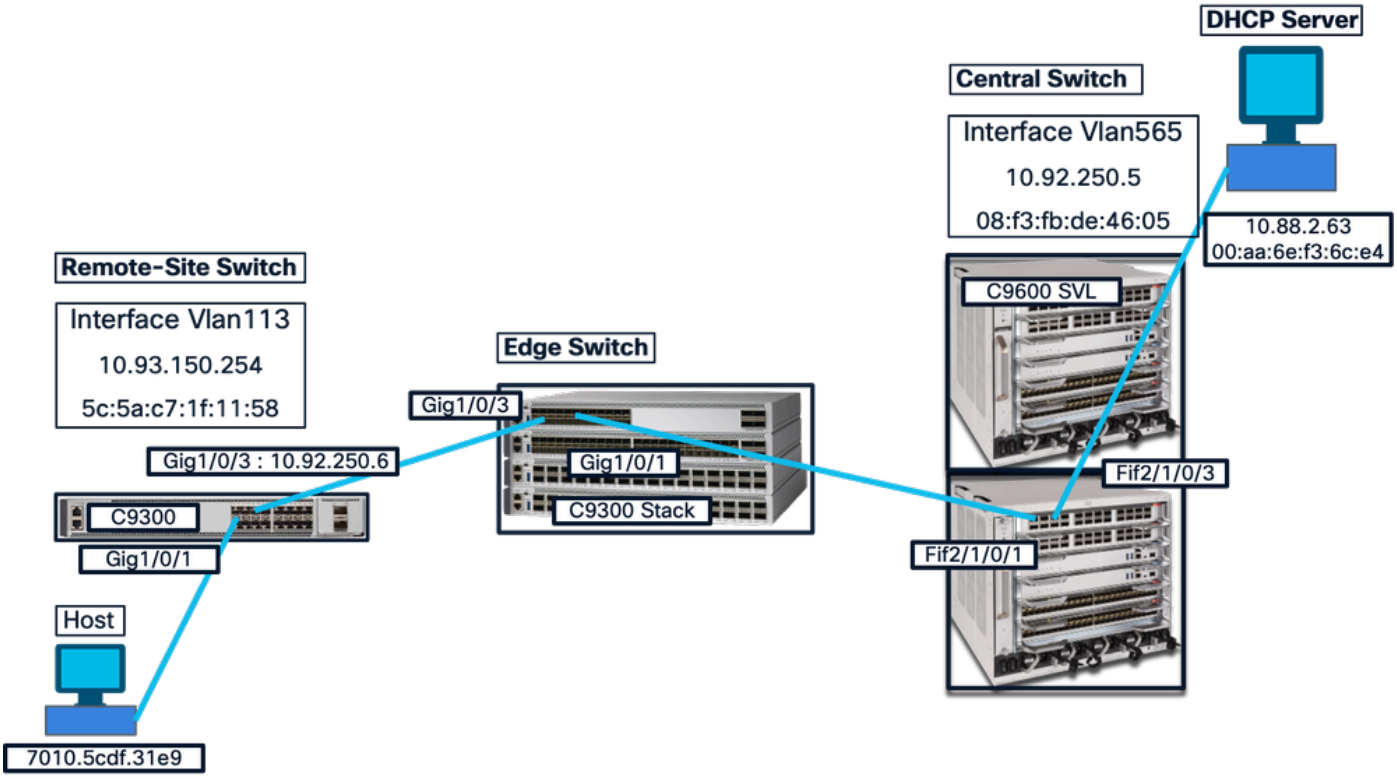
- Core/Distribution switch: Cisco Catalyst 9600X-reeks
- Access switch: Cisco Catalyst 9300-reeks
- DHCP-client: eindhostapparaat
- DHCP-server: gecentraliseerde netwerkserviceprovider

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

In dit document wordt onderzocht hoe DHCP-spionage DHCP-pakketten inspecteert en onderschept wanneer ze door een Layer 3-hop gaan. Met behulp van praktische configuratievoorbeelden en analyse van gerelateerde pakketopnames, demonstreert het de interactie van DHCP-snooping op Layer 3-hop binnen een netwerkomgeving van de Cisco Catalyst 9000-reeks.

Netwerkdiagram



Topologie

niet-werkend scenario

Ten eerste wordt het scenario beschreven waarin het DHCP Discover-pakket bij de Layer 3-hop wordt gedropt, met name op de Central Switch. Analyseer nu de pakketreis hop voor hop van de DHCP-client.

Switch-pakketverwerking op externe locatie

De host met MAC-adres 7010.5cdf.31e9 verzendt het DHCP Discover-pakket, dat aankomt bij GigabitEthernet1/0/1 op de switch op de externe locatie.

Externe siteconfiguratie

<#root>

!
!

Remote-Site#show run int vlan 113

```
Building configuration...

Current configuration : 170 bytes
!
interface Vlan113
ip address 10.93.150.254 255.255.255.0
ip helper-address 10.88.2.63
no ip redirects
no ip proxy-arp
end
!
!
!
```

Host Access Port

Remote-Site#show run int gig1/0/1

```
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet1/0/1
switchport access vlan 113
switchport mode access
end
!
!
!
```

Uplink Port

Remote-Site#show run int gig1/0/3

```
Building configuration...

Current configuration : 121 bytes
!
interface GigabitEthernet1/0/3
no switchport
ip address 10.92.250.6 255.255.255.252
end
!
!
```

Remote-Site#show run | sec dhcp

```
ip dhcp snooping vlan 1-999
no ip dhcp snooping information option
```

```
ip dhcp snooping
!
!
```

Remote-Site#show cdp neighbors

```
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

Edge-Switch   Gig 1/0/3        153          R S I         C9300-48H      Gig 1/0/3
!
!
```

Remote-Site#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.92.250.5 Gi1/0/3 14 00:04:40 1 100 0 20
!
!
```

Remote-Site#show ip route 10.88.2.63

```
Routing entry for 10.88.2.0/24
 Known via "eigrp 100", distance 90, metric 3072, precedence routine (0), type internal
 Redistributing via eigrp 100
 Last update from 10.92.250.5 on GigabitEthernet1/0/3, 00:05:15 ago
 Routing Descriptor Blocks:
 * 10.92.250.5, from 10.92.250.5, 00:05:15 ago, via GigabitEthernet1/0/3
     Route metric is 3072, traffic share count is 1
     Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
     Reliability 255/255, minimum MTU 1500 bytes
     Loading 1/255, Hops 1
!
!
```

Remote-site Switch Ingress

Het DHCP-detectiepakket uitzenden dat de switch op de externe site binnenkomt.

<#root>

```
!
!
```

Remote-Site#show monitor capture tac parameter

```
     monitor capture tac control-plane BOTH
     monitor capture tac interface GigabitEthernet1/0/1 BOTH
     monitor capture tac match any
     monitor capture tac file location flash:pcport.pcap
!
!
```

Remote-Site#show monitor capture file flash:pcport.pcap packet-number 667 detailed

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 667: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

```
Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
.... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
Source: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x0405 (1029)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
```

Protocol: UDP (17)

```
Header checksum: 0xb69d [validation disabled]
[Header checksum status: Unverified]
Source: 0.0.0.0
Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
```

Source Port: 68
Destination Port: 67
Length: 311
Checksum: 0x33de [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x000026ee
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)

Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!

```
!
```

Remote-site Switch Egress

Het Relayed Unicast DHCP Discover-pakket dat van Remote-site switch naar Edge Switch wordt afgesloten.

<#root>

```
!
!

Remote-Site#show monitor capture tac1 parameter


 monitor capture tac1 control-plane BOTH
 monitor capture tac1 interface GigabitEthernet1/0/3 BOTH
 monitor capture tac1 match any
 monitor capture tac1 file location flash:remote_edge.pcap
!
!

Remote-Site#show monitor capture file flash:pcport.pcap packet-number 669 detailed


Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 669: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)


Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63


0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
```

```
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x001c (28)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x0c94 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0xe48f [unverified]
[Checksum Status: Unverified]
[Stream index: 4]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x000026ee
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... .... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
```

Relay agent IP address: 10.93.150.254

```
Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
```

Option: (53) DHCP Message Type (Discover)

```
Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
```

```
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!
!
```

Opmerking: Het pakket met 'Relay Agent IP-adres: 10.93.150.254', maar het heeft geen DHCP Option 82 vanwege de configuratie 'geen ip dhcp snooping informatie optie' als onderdeel van de DHCP sectie.

Edge Switch-pakketverwerking

Edge switch is een L2-switch die alleen wordt gebruikt om de pakketjes van en naar de centrale/core-switch en de switches op de externe locatie te verdelen. Het vertrouwt alle DHCP-pakketten.

Edge Switch-configuratie

<#root>

```
!
!
```

Edge-Switch#show run int gig1/0/3

```
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/0/3
switchport access vlan 565
ip flow monitor IPv4_NETFLOW input
ip dhcp snooping trust
end
```

```
!
!
```

Edge-Switch#show run int gig1/0/1

```
Building configuration...

Current configuration : 119 bytes
!
interface GigabitEthernet1/0/1
switchport trunk native vlan 999
switchport mode trunk
ip dhcp snooping trust
end
!
!
```

Edge-Switch#show run | sec dhcp

```
ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
!
!
```

Edge-Switch#show cdp neighbors

```
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
Remote-Site      Gig 1/0/3       153       R S I        C9300L-48    Gig 1/0/3
Central-Switch   Gig 1/0/1       170       R S I        C9606R       Fif 2/1/0/1
!
!
```

Edge Switch Ingress

Het pakket dat van de Switch op de externe locatie wordt geëscorteerd, raakt de Edge-Switch zoals deze is.

Edge Switch Egress

Omdat dit een Layer 2 hop voor het pakket is, verlaat het de switch ongewijzigd als het doorgaat naar de volgende hop. De Edge-switch stuurt het pakketje door naar de Central-Switch zonder enige wijziging in het pakketje.

Edge Switch Egress Packet is het Ingress-pakket van Central Switch.

<#root>

```
!
!

Edge-Switch#show monitor capture tac parameters


 monitor capture tac control-plane BOTH
 monitor capture tac interface GigabitEthernet1/0/1 BOTH
 monitor capture tac match any
 monitor capture tac file location flash:edge_central.pcap
!
!

Edge-Switch#show monitor capture file flash:edge_central.pcap packet-number 25597 detail


Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 25597: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface /tmp/epc_ws/wif
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dhcp]

Ethernet II, Src: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)


Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63


0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x001c (28)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
```

Fragment offset: 0
Time to live: 255

Protocol: UDP (17)

Header checksum: 0x0c94 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0xe48f [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x000026ee
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List

```
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!
!
```

Central Switch Packet Processing

Configuratie van centrale Switch

<#root>

```
!
!

Central-Switch#show cdp neighbors


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

Edge-Switch    Fif 2/1/0/1     177       R S I        C9300-48H   Gig 1/0/1
!
!

Central-Switch#show run int fif2/1/0/1


Building configuration...

Current configuration : 115 bytes
!
interface FiftyGigE2/1/0/1
switchport trunk native vlan 999
switchport mode trunk
end
!
!
```

Central-Switch#show run int fif2/1/0/3

Building configuration...

Current configuration : 87 bytes
!
interface FiftyGigE2/1/0/3
no switchport
ip address 10.88.2.254 255.255.255.0
end
!
!

interface Vlan565

ip address 10.92.250.5 255.255.255.252
!
!
!

Central-Switch#show run | sec dhcp

ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
!
!

Central-Switch#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0

10.92.250.6

Vl565 11 00:10:32 3 100 0 19
~
~
!
!

router eigrp 100

  network 10.0.0.0
  network 10.88.0.0 0.0.255.255
  passive-interface default
  no passive-interface Vlan565
  eigrp router-id 10.255.255.254
!
!

Central Switch Ingress

Zoals eerder vermeld, Edge Switch Egress Packet is Central Switch Ingress-pakket.

Wanneer het pakket bij interface fif 2/1/0/1 aankomt, zal dit logboek worden waargenomen.

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-zero giaddr or optio
```

Interface Fif 2/1/0/1 is geconfigureerd als een niet-vertrouwde poort voor DHCP-snooping.

Via deze poort komt een Layer 3-gerelateerd DHCP Discover-pakket binnen. Hoewel het pakket wordt doorgestuurd en ingekapseld in Layer 3, inspecteert DHCP-snooping het nog steeds op de Layer 2-poort. Aangezien deze poort niet vertrouwd is en het pakket een Gateway IP-adres (Relay Agent) bevat zonder optie 82, zal DHCP-snooping het pakket op deze niet-vertrouwde poort laten vallen. Dit gedrag wordt verwacht en door ontwerp.

Opmerking: In veel van de gevallen wordt gezien dat DHCP Discover wordt gedropt in transit vanwege DHCP-snooping.

Central Switch Egress

In dit geval zal Central-Switch het DHCP Discover-pakket laten vallen en zal er geen DHCP Discover-pakket worden gestart door de host met MAC-adres 70:10:5c:df:31:e9 dat teruggaat van interface Fif 2/1/0/3.

Hoe het probleem oplossen?

1. Laat optie 82 ingeschakeld op de eerste hop van de DHCP-client.
Configureer in het huidige voorbeeld de opdracht ip dhcp snooping information option op de Remote-Switch.

2. Het vertrouwen in de DHCP-controle moet worden ingeschakeld op het hele DHCP-pad van DHCP-client naar DHCP-server.

Configureer in het huidige voorbeeld de opdracht ip dhcp snooping trust op interface fif2/1/0/1 van Central Switch.

<#root>

Central-Switch#show run int fif2/1/0/1

```
Building configuration...

Current configuration : 115 bytes
!
interface FiftyGigE2/1/0/1
switchport trunk native vlan 999
switchport mode trunk
```

ip dhcp snooping trust

```
end
```

Na deze wijzigingen zal het Discover-pakket van Central Switch naar de DHCP-server vertrekken.

<#root>

Frame 9: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dhcp]
```

Ethernet II, Src: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05), Dst: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)

```
Destination: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
Address: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63

```
0100 .... = Version: 4
```

.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x02ff (767)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 254
Protocol: UDP (17)
Header checksum: 0x0ab1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0x061b [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x00000563
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29

```
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
```

De Discover zal de DHCP-server bereiken en de DHCP-server zal de DHCP-aanbieding beantwoorden.

DHCP-aanbiedingspakket:

<#root>

Frame 128: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)

```
Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
Address: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.88.2.63, Dst: 10.93.150.254

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 339
Identification: 0x0006 (6)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 252
Protocol: UDP (17)
Header checksum: 0x0fa2 [validation disabled]
[Header checksum status: Unverified]
Source: 10.88.2.63
Destination: 10.93.150.254
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 319
Checksum: 0x9c4c [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
Bootstrap Protocol (Offer)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0

Your (client) IP address: 10.93.150.11

Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Offer)

```
Length: 1
DHCP: Offer (2)
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4
```

DHCP Server Identifier: 10.88.2.63

```
Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (73119s) 20 hours, 18 minutes, 39 seconds
Option: (58) Renewal Time Value
Length: 4
Renewal Time Value: (36559s) 10 hours, 9 minutes, 19 seconds
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (63973s) 17 hours, 46 minutes, 13 seconds
Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 8.8.8.8
Option: (255) End
Option End: 255
```

Het pakket met offertes dat door de DHCP-server wordt beantwoord, raakt de interface fif2/1/0/3 van CORE/Central Switch.

<#root>

Central-Switch#show run int fif2/1/0/3

```
Building configuration...

Current configuration : 87 bytes
!
interface FiftyGigE2/1/0/3
no switchport
ip address 10.88.2.254 255.255.255.0
end
```

Hier is er geen vertrouwen van DHCP-snuffelend en komt AANBIEDING binnen, waarom wordt de Aanbieding dan niet op een niet-vertrouwde poort gedropt?

Zoals u weet, in een netwerk waar DHCP Snooping is ingeschakeld, worden poorten gecategoriseerd als vertrouwd of niet-vertrouwd.

Vertrouwde poorten zijn verbonden met legitieme DHCP-servers of andere vertrouwde switches. Alle DHCP-berichten zijn toegestaan.
Niet-vertrouwde poorten zijn meestal verbonden met eindgebruikersapparaten (clients). Ze zijn beperkt om "DHCP Spoofing" of "Rogue DHCP Server" aanvallen te voorkomen.
DHCP-aanbod en DHCP ACK-pakketten worden beschouwd als 'server-side' berichten. Volgens de beveiligingsregels mogen deze berichten alleen afkomstig zijn van een legitieme server.
Wanneer een DHCP-relaisagent of een L3-router/Switch een DHCP-aanbieding ontvangt op een L2-poort die als niet-vertrouwd is geconfigureerd, wordt dit door het DHCP-snuffelmechanisme als een beveiligingsovertreding aangemerkt. Het veronderstelt dat een malafide DHCP-server probeert ongeautoriseerde IP-adressen te verstrekken aan clients in het netwerk.
Hoewel het pakket unicast is (specifiek gericht op de relay-agent), heeft de vertrouwensstatus van de fysieke of logische poort voorrang. De beveiligingscontrole wordt uitgevoerd op poortniveau, ongeacht of het pakket wordt uitgezonden of unicast.
Omdat de poort niet vertrouwd is, blokkeert het systeem het DHCP-aanbod om het netwerk te beschermen tegen mogelijk schadelijke of onjuiste configuratiegegevens die afkomstig zijn van een niet-geautoriseerde bron.

Een L3-poort (een gerouteerde interface) werkt op Layer 3. Omdat het een gerouteerde interface is, houdt het zich niet aan de L2 DHCP Snooping trust / untrust-regels die van toepassing zijn op switchports.
Een klant stuurt een uitzendverzoek. De Relay Agent (het L3-apparaat) onderschept dit en stuurt een unicast-verzoek naar de DHCP-server.
De DHCP-server stuurt een unicast DHCP-aanbod terug naar het IP-adres van de Relay Agent (met name naar het IP-adres van de gateway of gateway).
Wanneer het pakket aankomt op de L3-poort van de Relay Agent of op een L3-hop in het pakketpad, accepteert het apparaat het pakket als legitiem routeringsverkeer.
In tegenstelling tot het eerdere scenario (een L2 niet-vertrouwde poort), waarbij de switch op zoek is naar 'server-side' berichten afkomstig van een client-facing poort, fungeert de L3-poort als de beoogde bestemming of legitieme L3-hop voor de reactie van de server.
Als L3-poorten unicast DHCP-aanbiedingen hebben laten vallen, zal het DHCP-relayingmechanisme nooit werken, omdat de server nooit in staat zal zijn om terug te communiceren naar de relay-agent.

Uiteindelijk zal het Aanbiedingspakket doorlopen totdat het de klant bereikt.

De host/client antwoordt terug met DHCP-verzoek.

Frame 20: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0

~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....1 .... = IG bit: Group address (multicast/broadcast)
Source: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 349
Identification: 0x3be5 (15333)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x7eab [validation disabled]
[Header checksum status: Unverified]
Source: 0.0.0.0
Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 329
Checksum: 0xed98 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563

Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Request)

Length: 1
DHCP: Request (3)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63

Option: (50) Requested IP Address
Length: 4

Requested IP Address: 10.93.150.11

Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (73119s) 20 hours, 18 minutes, 39 seconds
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier

```
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
```

DHCP-server zal eindelijk de toewijzing van het IP-adres ACK.

<#root>

Frame 25: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05), Dst: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)

```
Destination: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.88.2.63, Dst: 10.93.150.254

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 339
Identification: 0x0007 (7)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 252
Protocol: UDP (17)
Header checksum: 0x0fa1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.88.2.63
Destination: 10.93.150.254
User Datagram Protocol, Src Port: 67, Dst Port: 67
```

Source Port: 67
Destination Port: 67
Length: 319
Checksum: 0x1e0f [unverified]
[Checksum Status: Unverified]
[Stream index: 2]

Bootstrap Protocol (ACK)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0

Your (client) IP address: 10.93.150.11

Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (ACK)

Length: 1
DHCP: ACK (5)
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63

Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (86400s) 1 day

```
Option: (58) Renewal Time Value
Length: 4
Renewal Time Value: (43200s) 12 hours
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (75600s) 21 hours
Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 8.8.8.8
Option: (255) End
Option End: 255
```

DORA voltooit en de host ontvangt het IP-adres met succes.

Samenvatting

Raadpleeg deze tabel om de scenario's voor het doorsturen van pakketten te begrijpen.

Poorttype	vertrouwensstatus	Gerelateerd pakkettype	resultaat	reden
L2-poort	onbetrouwbaar	Unicast DHCP-aanbieding/ACK	gevallen	DHCP Snooping voorkomt serverberichten op niet-vertrouwde L2-poorten.
L3-poort	N.v.t. (gerouteerd)	Unicast DHCP-aanbieding/ACK	aanvaard	Gerouteerde poorten zijn de beoogde knooppunten voor Relay Agent-communicatie.
L2-poort	vertrouwd	Unicast DHCP Discover met optie 82	aanvaard	Vertrouwde poort maakt alle DHCP-signalen mogelijk.
L2-poort	onbetrouwbaar	Unicast DHCP Discover met optie 82	aanvaard	Het pakket met het IP-adres van de relay-agent en optie 82 is legitiem.
L2-poort	vertrouwd	Unicast DHCP Discover zonder optie 82	aanvaard	Vertrouwde poort maakt alle DHCP-signalen mogelijk.
L2-poort	onbetrouwbaar	Unicast DHCP Discover	gevallen	Het pakket met het IP-adres van

		zonder optie 82		de relay-agent en geen optie 82 is bedrieglijk.

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.