

DHCP-Snooping-Interaktionen mit GIADDR und Option 82 auf CAT9000

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwermdiagramm](#)

[Testfälle](#)

[DHCP-Snooping für Core-Switch aktiviert](#)

[Access Switch-Option 82 deaktiviert](#)

[Access Switch-Option 82 aktiviert](#)

[DHCP-Snooping für Core-Switch deaktiviert](#)

[Access Switch-Option 82 aktiviert](#)

[Access Switch-Option 82 deaktiviert](#)

[Zusammenfassung](#)

Einleitung

Dieses Dokument beschreibt die DHCP-Snooping-Interaktionen mit GIADDR und Option 82 auf CAT9000.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS® XE Kenntnisse in Konfiguration und Betriebsbefehlen.
- Vertrautheit mit der Hardware und Architektur von Cisco Catalyst Switches der Serie 9000
- Grundlegendes Verständnis der DHCP-Protokollvorgänge und DHCP-Snooping-Mechanismen
- Grundlegendes Verständnis der DHCP-Option 82 und der Rolle des Relay-Agenten

Verwendete Komponenten

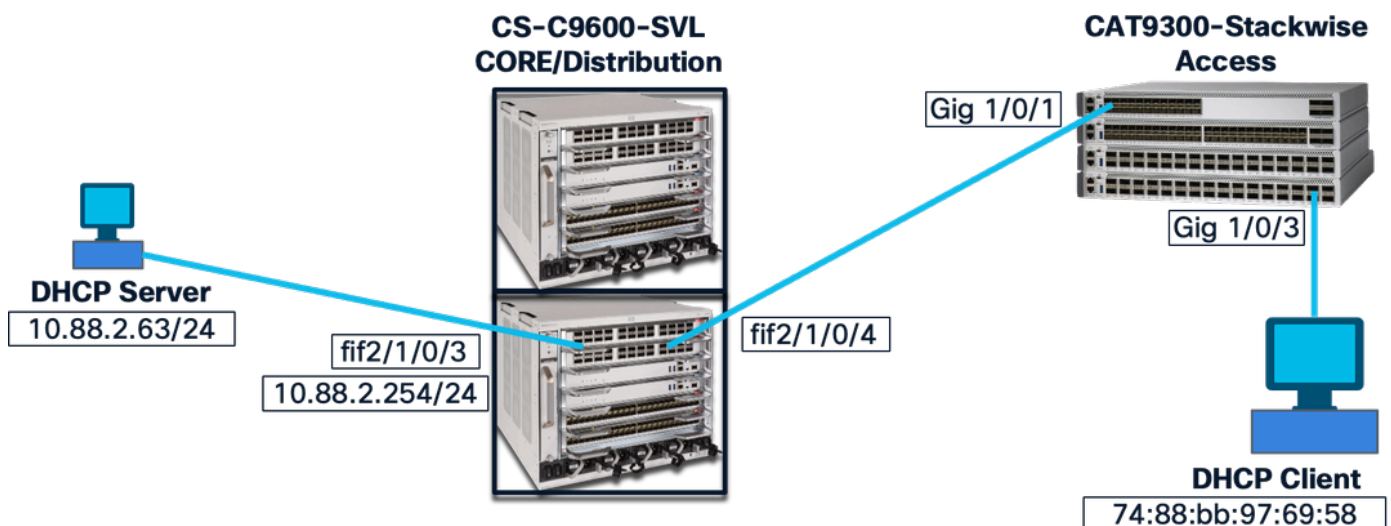
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Core/Distribution Switch: Cisco Catalyst Serie 9600X
- Access Switch: Cisco Catalyst Serie 9300
- DHCP-Client: Endhost-Gerät
- DHCP-Server: zentraler Netzwerkdienstanbieter

Hintergrundinformationen

In diesem Dokument werden verschiedene Konfigurationen von DHCP-Snooping auf Core-/Distribution-Switches untersucht, die mit DHCP-Option 82-Implementierungen auf Access-Switches integriert sind. Durch praktische Konfigurationsbeispiele und die Analyse der entsprechenden Paketerfassungen veranschaulicht dieser Leitfaden die Interaktion zwischen diesen Funktionen in einer Umgebung mit Cisco Catalyst Switches der Serie 9000.

Netzwerkdiagramm



Testfälle

DHCP-Snooping für Core-Switch aktiviert

Access Switch-Option 82 deaktiviert

Core-Switch:

```
<#root>
!
int f1f2/1/0/4 --> Downlink to Access Switch
ip dhcp snooping trust
!
ip dhcp snooping vlan 1-2048

ip dhcp snooping

!
```

Access Switch:

```
<#root>
!
int gig1/0/1 -> uplink to Core
ip dhcp snooping trust
switchport mode trunk
!
ip dhcp snooping vlan 1-1400

no ip dhcp snooping information option

ip dhcp snooping
!
int gig1/0/3 ----> End device connected port
switchport mode access
switchport access vlan 287
!
```

Ergebnis:

Erfolgreich

Das Endgerät erhält die IP-Adresse ohne Probleme.

Erläuterung:

Access Switch Option 82 ist deaktiviert und sendet das Paket an den Kern ohne Option 82. Core Switch Option 82 ist standardmäßig aktiviert und fügt die Option 82 mit der IP-Adresse des Relay-Agenten im Paket hinzu und sendet es an den DHCP-Server.

Paket an Verbindung zwischen Client und Access Switch:

No.	Time	Source	Destination	Protoco	Lengt	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID 0x1604
2	0.000156	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID 0x1604
3	2.002663	10.88.39.254	255.255.255.255	DHCP	363	DHCP Offer - Transaction ID 0x1604
4	2.002977	10.88.39.254	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x1604
5	2.004966	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID 0x1604
6	2.005228	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID 0x1604
7	2.007080	10.88.39.254	255.255.255.255	DHCP	363	DHCP ACK - Transaction ID 0x1604


```
> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmp/epc_v
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00001604
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End
```



Anmerkung: Die Paketerfassung wird mehrmals und an mehreren Erfassungspunkten für denselben Client durchgeführt. ignorieren Sie daher die Transaktions-ID.

Paket an Verbindung zwischen Access Switch und Distribution/Core-Switch:

Der Access Switch verfügt nicht über die Einfügung einer Snooping-Informationsoption, sodass dasselbe Paket vom Client an den Distribution Switch weitergeleitet wird.

No.	Time	Source	Destination	Protocol	Length	Info
5	11.360258	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID 0x1147
6	12.858224	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8478fad8
7	12.858519	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8478fad8
8	13.362861	10.88.39.254	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x1147
9	13.364854	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID 0x1147
10	13.469795	10.88.39.254	255.255.255.255	DHCP	359	DHCP ACK - Transaction ID 0x1147

```

> Frame 5: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmp/epc_ws.
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00001147
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Paket zwischen CORE-Switch und DHCP-Server:

Wenn DHCP-Snooping aktiviert und ein Relay konfiguriert ist, wird der CORE-Switch, der das Paket per Unicasting an den DHCP-Server 10.88.2.63 mit Relay-Agent-IP sendet, als eigene IP eingefügt.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.88.39.254	10.88.2.63	DHCP	379	DHCP Discover - Transaction ID 0x5df
2	0.000069	10.88.2.63	10.88.39.254	DHCP	359	DHCP Offer - Transaction ID 0x5df
3	0.128743	10.88.39.254	10.88.2.63	DHCP	397	DHCP Request - Transaction ID 0x5df
4	0.128997	10.88.2.63	10.88.39.254	DHCP	359	DHCP ACK - Transaction ID 0x5df


```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmp/epc_
> Ethernet II, Src: Cisco_de:46:05 (08:f3:fb:de:46:05), Dst: Cisco_f3:6c:e4 (00:aa:6e:f3:6c:e4)
> Internet Protocol Version 4, Src: 10.88.39.254, Dst: 10.88.2.63
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000005df
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: 10.88.39.254
  Client MAC address: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Access Switch-Option 82 aktiviert

Core-Switch:

<#root>

```

!
int fif2/1/0/4 --> Downlink to Access Switch
ip dhcp snooping trust
!
ip dhcp snooping vlan 1-2048

ip dhcp snooping
!

```

Access Switch:

<#root>

```
!  
int gig1/0/1 -> uplink to Core  
ip dhcp snooping trust  
switchport mode trunk  
!  
ip dhcp snooping vlan 1-1400  
  
ip dhcp snooping information option
```

```
ip dhcp snooping  
!  
int gig1/0/3  
switchport mode access  
switchport access vlan 287  
!
```

Ergebnis:

Erfolgreich

Das Endgerät erhält die IP-Adresse ohne Probleme.

Erläuterung:

Access Switch-Option 82 ist aktiviert, aber dieser Switch hat keine SVI erstellt und sendet das Paket ohne Option 82 an den Kern. Core Switch-Option 82 ist standardmäßig aktiviert und fügt die Option 82 mit der IP-Adresse des Relay Agents im Paket hinzu und sendet es an den DHCP-Server.

Paket vom Client zum Access Switch:

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID
2	0.000161	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID
3	1.110008	Cisco_9e:c8:c6	Broadcast	ARP	64	Who has 10.88.0.254? Tell 10.88
4	2.002486	10.88.39.254	255.255.255.255	DHCP	383	DHCP Offer - Transaction ID
5	2.002871	10.88.39.254	255.255.255.255	DHCP	379	DHCP Offer - Transaction ID
6	2.004750	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID
7	2.004994	0.0.0.0	255.255.255.255	DHCP	417	DHCP Request - Transaction ID
8	2.006887	10.88.39.254	255.255.255.255	DHCP	383	DHCP ACK - Transaction ID
9	2.108976	10.88.39.254	255.255.255.255	DHCP	379	DHCP ACK - Transaction ID

```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00000121
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Das Paket vom Access Switch zum Core/Distribution Switch:

Da die Option "ip dhcp snooping information option" auf dem Access Switch standardmäßig aktiviert ist, fügt der Access Switch die Option 82 mit der Relay-IP-Adresse 0.0.0.0 ein.

Laut DHCP Snooping World handelt es sich um ein unautorisiertes Paket, das vom CORE-Switch verworfen werden muss. Da dem CORE-Switch die Schnittstelle jedoch als vertrauenswürdig gilt, wird das Paket für die Weiterleitung an den DHCP-Server verarbeitet.

Time	Source	Destination	Protocol	Length	Info
2 0.000129	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction I
3 0.002398	10.88.39.254	255.255.255.255	DHCP	379	DHCP Offer - Transaction I
4 0.005010	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction I

```

> Frame 2: Packet, 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000026a5
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  v Option: (82) Agent Information Option
    Length: 18
    v Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 0004011f0103
    v Option 82 Suboption: (2) Agent Remote ID
      Length: 8
      Agent Remote ID: 000690eb5000eb80
  v Option: (255) End
    Option End: 255

```

Paket zwischen CORE-Switch und DHCP-Server:

Da die Downlink-Schnittstelle vertrauenswürdig ist, ersetzt der CORE-Switch den Relay-Agenten von 0.0.0.0 bis 10.88.39.254 und sendet diesen an den Uplink.

Der DORA-Prozess wird legitimiert und der Client erhält die IP-Adresse.

Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.88.39.254	10.88.2.63	DHCP	399 DHCP Discover - Transaction ID 0x9fc
2	2.000064	10.88.2.63	10.88.39.254	DHCP	379 DHCP Offer - Transaction ID 0x9fc
3	2.003716	10.88.39.254	10.88.2.63	DHCP	417 DHCP Request - Transaction ID 0x9fc
4	2.003963	10.88.2.63	10.88.39.254	DHCP	379 DHCP ACK - Transaction ID 0x9fc

```

> Frame 1: Packet, 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface /t
> Ethernet II, Src: Cisco_de:46:05 (08:f3:fb:de:46:05), Dst: Cisco_f3:6c:e4 (00:aa:6e:f3:6c:e4)
> Internet Protocol Version 4, Src: 10.88.39.254, Dst: 10.88.2.63
> User Datagram Protocol, Src Port: 67, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000009fc
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: 10.88.39.254
  Client MAC address: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  < Option: (82) Agent Information Option
    Length: 18
    < Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 0004011f0103
    < Option 82 Suboption: (2) Agent Remote ID
      Length: 8
      Agent Remote ID: 000690eb5000eb80
    > Option: (255) End
  
```

DHCP-Snooping für Core-Switch deaktiviert

Access Switch-Option 82 aktiviert

Core-Switch:

```
<#root>
```

```
!
Int fif2/1/0/4 --> Downlink to Access Switch
no Ip dhcp snooping trust
!
```

```
no ip dhcp snooping vlan 1-2048
```

```
no ip dhcp snooping
```

```
!
```

Access Switch:

```
<#root>
```

```
!  
int gig1/0/1 -> uplink to Core  
ip dhcp snooping trust  
switchport mode trunk  
!  
ip dhcp snooping vlan 1-1400
```

```
ip dhcp snooping information option
```

```
ip dhcp snooping  
!  
int gig1/0/3  
switchport mode access  
switchport access vlan 287  
!
```

Ergebnis:

Fehler.

Das Endgerät erhält die IP-Adresse nicht.

Erläuterung:

Die Access Switch-Option 82 ist aktiviert, dieser Switch verfügt jedoch weder über SVI noch über einen Relay Agent. Daher sendet er das Paket an den CORE mit Option 82 und Relay IP als 0.0.0.0. Da DHCP Snooping auf dem CORE Switch deaktiviert ist die Überprüfung, Bearbeitung und Einfügung von Option 82 ist dort deaktiviert. Der CORE-Switch fügt das Relay nicht hinzu und verwirft das Paket.

Client DHCP erkennt das Paket, das vom Client eingeht und an den Access Switch übergeht:

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID
2	0.000187	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID
3	3.223897	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID
4	7.224730	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID

```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
√ Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00001617
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Paketfluss vom Access Switch zum Core/Distribution Switch:

- Auf dem Access Switch ist der Befehl `ip dhcp snooping information` aktiviert, wodurch die Option 82 in DHCP-Pakete eingefügt wird. In diesem Fall wird die IP-Adresse des Relay-Agenten in Option 82 auf 0.0.0.0 festgelegt.
- Der Access Switch arbeitet ausschließlich auf Layer 2 für vLAN 287.
- Aus Sicht des CORE-Switches wird das Paket mit der Option 82, das vom Access Switch eingefügt wird, als illegitim betrachtet. Da jedoch die Downlink-Schnittstelle auf dem CORE-Switch als vertrauenswürdig konfiguriert ist, verarbeitet der CORE-Switch das Paket, anstatt es auf Schnittstellenebene zu verwerfen.
- Auf dem CORE-Switch ist DHCP-Snooping deaktiviert, daher werden Pakete mit Option 82 nicht weitergeleitet.

CORE-Switch-Verhalten bei DHCP-Ermittlungspaketen:

- Der CORE-Switch versucht, das DHCP-Ermittlungspaket mit der konfigurierten Helper-Adresse 10.88.2.63 zu entschlüsseln.
- Dazu muss der CORE-Switch die Relay-IP-Adresse (GIADDR) im DHCP-Paket festlegen.
- Da Option 82 bereits vorhanden ist und Daten vom Access Switch eingefügt wurden, muss der CORE Switch Option 82 überprüfen, bevor die Relay-IP-Adresse festgelegt wird.
- Da DHCP-Snooping auf dem CORE-Switch deaktiviert ist, kann Option 82 nicht überprüft werden.
- Da Option 82 nicht überprüft und geändert werden kann, hat der CORE-Switch keine andere Wahl, als das DHCP-Ermittlungspaket zu verwerfen.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0
2 3.974135	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0
3 7.075635	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0

```

> Frame 1: Packet, 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000018b1
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 0000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  < Option: (82) Agent Information Option
    Length: 18
    < Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 0004011f0103
    < Option 82 Suboption: (2) Agent Remote ID
      Length: 8
      Agent Remote ID: 000690eb5000eb80
  > Option: (255) End

```

Das Ermittlungspaket wird nicht vom CORE-Switch zum DHCP-Server weitergeleitet.

Fehlerbehebung am CORE-Switch bei nicht funktionierenden Szenarien:

```
DHCPD: Reload workspace interface Vlan287 tableid 0.  
DHCPD: tableid for 10.88.39.254 on Vlan287 is 0  
DHCPD: client's VPN is .  
DHCPD: No option 125  
DHCPD: Option 124: Vendor Class Information  
DHCPD: Enterprise ID: 9  
DHCPD: Vendor-class-data-len: 13  
DHCPD: Data: 43~~~~~58  
DHCPD: inconsistent relay information.  
DHCPD: relay information option exists, but giaddr is zero.
```

Access Switch-Option 82 deaktiviert

Core-Switch:

```
<#root>
```

```
!  
int fif2/1/0/4 --> Downlink to Access Switch  
no ip dhcp snooping trust  
!  
no ip dhcp snooping vlan 1-2048  
  
no ip dhcp snooping
```

```
!
```

Access Switch:

```
!  
int gig1/0/1 -> uplink to Core  
ip dhcp snooping trust  
switchport mode trunk  
!  
ip dhcp snooping vlan 1-1400  
no ip dhcp snooping information option  
ip dhcp snooping  
!  
int gig1/0/3  
switchport mode access  
switchport access vlan 287  
!
```

Ergebnis:

Erfolgreich

Das Endgerät erhält die IP-Adresse.

Beobachtung:

Access Switch-Option 82 ist deaktiviert und sendet das Paket ohne Option 82 an den Kern. Für den CORE Switch ist die SVI vorhanden, und das Relay ist konfiguriert. Der CORE-Switch fügt die IP-Adresse des Relay-Agents dem Paket hinzu und sendet sie an den DHCP-Server.

Client-DHCP erkennt Pakete, die auf den Access Switch eintreffen:

Time	Source	Destination	Protocol	Length	Info
6	11.127914	0.0.0.0	255.255.255.255	DHCP	379 DHCP Discover - Transaction ID
7	12.467192	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID
8	12.467511	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID
9	13.130633	10.88.39.254	255.255.255.255	DHCP	359 DHCP Offer - Transaction ID
10	13.132841	0.0.0.0	255.255.255.255	DHCP	397 DHCP Request - Transaction ID
11	13.236938	10.88.39.254	255.255.255.255	DHCP	359 DHCP ACK - Transaction ID

```

> Frame 6: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00002336
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Paket-zu-CORE-Switch vom Access Switch:

Wenn Option 82 auf dem Access Switch deaktiviert ist, leitet der Access Switch das Broadcast-Paket wie auf dem Uplink-Trunk weiter.

Time	Source	Destination	Protocol	Length	Info
6	10.652455	0.0.0.0	255.255.255.255	DHCP	379 DHCP Discover - Transaction ID
7	11.292839	Cisco_9e:c8:c6	Broadcast	ARP	64 Who has 10.88.0.254? Tell 10.8
8	12.653654	10.88.39.254	255.255.255.255	DHCP	359 DHCP Offer - Transaction ID
9	12.655561	0.0.0.0	255.255.255.255	DHCP	397 DHCP Request - Transaction ID
10	12.655730	0.0.0.0	255.255.255.255	DHCP	397 DHCP Request - Transaction ID
11	12.760079	10.88.39.254	255.255.255.255	DHCP	359 DHCP ACK - Transaction ID

```

> Frame 6: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000003fd
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Paket wird vom CORE-Switch zum DHCP-Server weitergeleitet:

Time	Source	Destination	Protocol	Length	Info
1 0.000000	10.88.39.254	10.88.2.63	DHCP	379	DHCP Discover - Transaction ID 0x271
2 0.000139	10.88.2.63	10.88.39.254	DHCP	359	DHCP Offer - Transaction ID 0x271
3 0.463381	10.88.39.254	10.88.2.63	DHCP	397	DHCP Request - Transaction ID 0x271
4 0.463628	10.88.2.63	10.88.39.254	DHCP	359	DHCP ACK - Transaction ID 0x271

```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmj
> Ethernet II, Src: Cisco_de:46:05 (08:f3:fb:de:46:05), Dst: Cisco_f3:6c:e4 (00:aa:6e:f3:6c:e4)
> Internet Protocol Version 4, Src: 10.88.39.254, Dst: 10.88.2.63
> User Datagram Protocol, Src Port: 67, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x00000271
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: 10.88.39.254
  Client MAC address: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Fehlerbehebung am CORE-Switch:

```

Option 82 not present
DHCPD: Reload workspace interface Vlan287 tableid 0.
DHCPD: tableid for 10.88.39.254 on Vlan287 is 0
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: No option 124
DHCPD: FSM state change INVALID
DHCPD: Workspace state changed from INIT to INVALID
DHCPD: Finding a relay for client ~~~~ on interface Vlan287.
DHCPD : Locating relay for Subnet 10.88.39.254
DHCPD: there is no pool for 10.88.39.254.
DHCPD: Looking up binding using address 10.88.39.254
DHCPD: setting giaddr to 10.88.39.254

```

In diesem Fall erhält der Client die IP-Adresse.

Zusammenfassung

- DHCP-Snooping muss aktiviert sein, damit der Switch Informationen zu DHCP-Option 82 einfügen, entfernen oder validieren kann.
- Wenn DHCP-Snooping deaktiviert ist, führt der Switch die Einfüge- oder Entfernungsfunktionen der Option 82 nicht aus.
- Die Verarbeitung von Option 82, einschließlich des Löschens oder Zulassen von Paketen mit Option 82, hängt von der Aktivierung und Konfiguration von DHCP-Snooping ab.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.