

Informazioni sullo snooping DHCP per i pacchetti che attraversano gli hop di livello 3

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Scenario non lavorativo](#)

[Elaborazione pacchetti switch sito remoto](#)

[Configurazione sito remoto](#)

[Ingresso switch sito remoto](#)

[Uscita switch sito remoto](#)

[Elaborazione pacchetti Edge Switch](#)

[Configurazione Edge Switch](#)

[Edge Switch in ingresso](#)

[Uscita Edge Switch](#)

[Elaborazione pacchetti switch centrale](#)

[Configurazione switch centrale](#)

[Switch in ingresso centrale](#)

[Uscita switch centrale](#)

[Come risolvere il problema?](#)

[Riepilogo](#)

Introduzione

Questo documento descrive le interazioni e il comportamento dello snooping DHCP quando il pacchetto attraversa un dispositivo L3 e se il pacchetto è incapsulato nell'intestazione L3.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Competenza Cisco IOS® XE nella configurazione e nei comandi operativi.
- Familiarità con l'hardware e l'architettura dello switch Cisco Catalyst serie 9000.
- Comprensione approfondita delle operazioni del protocollo DHCP e dei meccanismi di snooping DHCP.
- Comprensione concettuale dell'opzione DHCP 82 e del ruolo dell'agente di inoltra.
- Conoscenze base del protocollo di routing.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

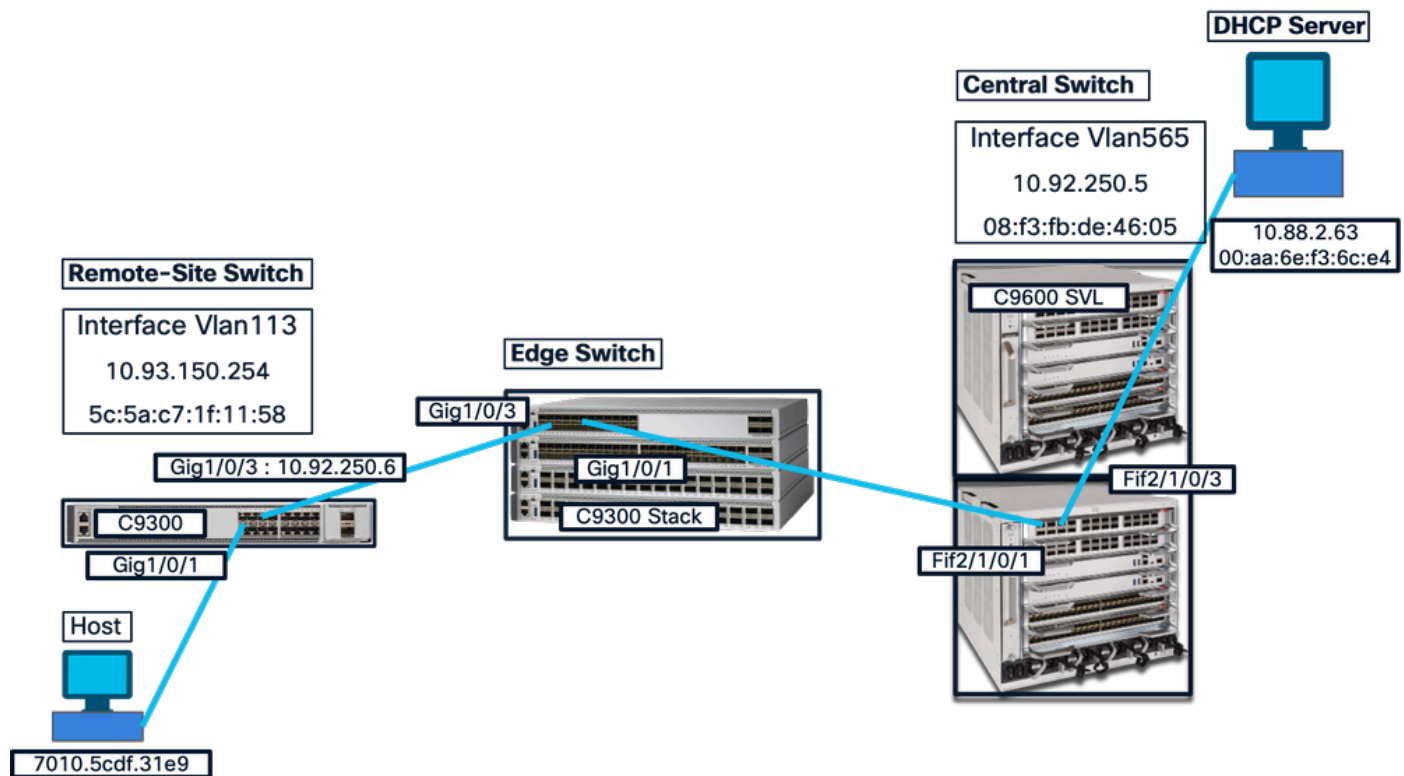
- Switch Core/distribuzione: Cisco Catalyst serie 9600X
- Switch di accesso: Cisco Catalyst serie 9300
- Client DHCP: Dispositivo host finale
- Server DHCP: Provider di servizi di rete centralizzato

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene esaminato come lo snooping DHCP controlla e intercetta i pacchetti DHCP quando attraversano un hop di layer 3. Utilizzando esempi pratici di configurazione e analisi delle acquisizioni di pacchetti correlate, mostra l'interazione dello snooping DHCP sugli hop di layer 3 in un ambiente di rete Cisco Catalyst serie 9000.

Esempio di rete



Topologia

Scenario non lavorativo

In primo luogo, viene descritto lo scenario in cui il pacchetto DHCP Discover viene scartato all'hop di layer 3, in particolare sullo switch centrale. A questo punto, analizzare il percorso del pacchetto hop dopo hop dal client DHCP.

Elaborazione pacchetti switch sito remoto

L'host con indirizzo MAC 7010.5cdf.31e9 trasmette il pacchetto DHCP Discover, che arriva all'interfaccia Gigabit Ethernet1/0/1 sullo switch del sito remoto.

Configurazione sito remoto

```
<#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
!
!

Ingresso switch sito remoto

Il pacchetto di individuazione DHCP broadcast entra nello switch del sito remoto.

<#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
!

!

Uscita switch sito remoto

Il pacchetto di individuazione DHCP unicast inoltrato sta uscendo dallo switch del sito remoto allo switch Edge.

<#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
!
!
```



Nota: Il pacchetto ha 'Indirizzo IP agente di inoltro:10.93.150.254' ma non ha l'opzione DHCP 82 a causa della configurazione 'no ip dhcp snooping information option' come parte della sezione DHCP.

Elaborazione pacchetti Edge Switch

Per il flusso DHCP motivo di preoccupazione, lo switch Edge è uno switch L2 utilizzato solo per distribuire i pacchetti da e verso lo switch centrale/di base e gli switch del sito remoto. Considera attendibili tutti i pacchetti DHCP.

Configurazione Edge Switch

```
<#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 in ingresso

Il pacchetto in uscita dallo switch del sito remoto sta raggiungendo lo switch senza apportare modifiche.

Uscita Edge Switch

Poiché si tratta di un hop di layer 2 per il pacchetto, esce dallo switch senza modifiche mentre procede all'hop successivo. Il dispositivo Edge-switch inoltra il pacchetto allo switch centrale senza apportare alcuna modifica al pacchetto.

Il pacchetto di uscita di Edge Switch è il pacchetto in entrata di 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
!
!

```

Elaborazione pacchetti switch centrale

Configurazione switch centrale

```
<#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  
!  
!
```

Switch in ingresso centrale

Come accennato in precedenza, il pacchetto di uscita dello switch edge è il pacchetto in entrata dello switch centrale.

Quando il pacchetto arriva all'interfaccia fif 2/1/0/1, viene osservato questo log.

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

L'interfaccia Fif 2/1/0/1 è configurata come porta non attendibile per lo snooping DHCP.

Tramite questa porta viene immesso un pacchetto di individuazione DHCP di layer 3 inviato. Anche se il pacchetto viene inoltrato e incapsulato al layer 3, lo snooping DHCP lo controlla ancora sulla porta di layer 2. Poiché questa porta non è attendibile e il pacchetto contiene un indirizzo IP gateway (agente di inoltro) senza l'opzione 82, lo snooping DHCP scarta il pacchetto su questa porta non attendibile. Questo comportamento è previsto e previsto.



Nota: In molti casi, è possibile notare che il rilevamento DHCP viene interrotto a causa dello snooping DHCP.

Uscita switch centrale

In questo caso, lo switch centrale scarta il pacchetto DHCP Discover e non vi è alcun pacchetto DHCP Discover avviato dall'host con indirizzo MAC 70:10:5c:df:31:e9 in uscita dall'interfaccia Fif 2/1/0/3.

Come risolvere il problema?

1. Attivare l'opzione 82 sul primo hop del client DHCP.

Nell'esempio corrente, configurare il comando `ip dhcp snooping information option` sullo switch remoto.

2. Il trust di snooping DHCP deve essere abilitato per tutto il percorso DHCP dal client DHCP al server DHCP.

Nell'esempio corrente, configurare il comando ip dhcp snooping trust sull'interfaccia fif2/1/0/1 dello switch centrale.

<#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

Dopo queste modifiche, il pacchetto di individuazione inizierà a partire dallo switch centrale verso il server DHCP.

<#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

Il comando Discover raggiungerà il server DHCP e il server DHCP risponderà all'offerta DHCP.

Pacchetto offerta DHCP:

<#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

Il pacchetto dell'offerta a cui il server DHCP ha risposto invierà un messaggio di errore sull'interfaccia fif2/1/0/3 dello switch CORE/Central.

<#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

Qui non c'è fiducia dall'estremità dello snooping DHCP e l'offerta sta entrando, allora perché l'offerta non viene scartata su una porta non attendibile?

Come è noto, in una rete in cui lo snooping DHCP è abilitato, le porte vengono classificate come attendibili o non attendibili.

Le porte attendibili sono connesse a server DHCP o ad altri switch attendibili. Tutti i messaggi DHCP sono consentiti.

Le porte non attendibili sono in genere connesse a dispositivi dell'utente finale (client). Sono limitati per prevenire attacchi di tipo "spoofing DHCP" o "server DHCP non autorizzati".

I pacchetti dell'offerta DHCP e dell'ACK DHCP sono considerati messaggi sul lato server. In base alle regole di protezione, questi messaggi devono provenire solo da un server legittimo.

Quando un agente di inoltro DHCP o un router/switch L3 riceve un'offerta DHCP su una porta L2 configurata come non attendibile, il meccanismo di snooping DHCP la considera una violazione della sicurezza. Si presume che un server DHCP non autorizzato stia tentando di fornire indirizzi IP non autorizzati ai client della rete.

Anche se il pacchetto è unicast (diretto in modo specifico all'agente di inoltro), lo stato di attendibilità della porta fisica o logica ha la precedenza. Il controllo di sicurezza viene eseguito a livello di porta indipendentemente dal fatto che il pacchetto sia broadcast o unicast.

Poiché la porta non è attendibile, il sistema bloccherà l'offerta DHCP per proteggere la rete da dati di configurazione potenzialmente dannosi o non corretti provenienti da un'origine non autorizzata.

Una porta L3 (un'interfaccia instradata) funziona sul layer 3. Trattandosi di un'interfaccia instradata, non rispetta le regole di attendibilità/non attendibilità dello snooping DHCP L2 applicabili alle porte switch.

Un client invia una richiesta di trasmissione. L'agente di inoltro (il dispositivo L3) intercetta questa condizione e invia una richiesta unicast al server DHCP.

Il server DHCP invia un'offerta DHCP unicast all'indirizzo IP dell'agente di inoltro (in particolare all'indirizzo IP del gateway o del server di inoltro).

Quando il pacchetto arriva alla porta L3 dell'agente di inoltro o a un hop L3 nel percorso del pacchetto, il dispositivo accetta il pacchetto come traffico di routing legittimo.

A differenza dello scenario precedente (una porta L2 non attendibile), in cui lo switch cerca messaggi sul lato server provenienti da una porta sul client, la porta L3 funge da destinazione prevista o da hop L3 legittimo per la risposta del server.

Se le porte L3 eliminano le offerte DHCP unicast, il meccanismo di inoltro DHCP non funzionerà mai, in quanto il server non sarà mai in grado di comunicare con l'agente di inoltro.

Infine, il pacchetto dell'offerta attraverserà il client finché non raggiunge quest'ultimo.

L'host/client risponderà con la richiesta DHCP.

<#root>

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

Il server DHCP eseguirà il ACK dell'assegnazione dell'indirizzo IP.

<#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 viene completato e l'host riceverà l'indirizzo IP correttamente.

Riepilogo

Per informazioni sugli scenari di inoltro dei pacchetti, fare riferimento a questa tabella.

Tipo porta	Stato trust	Tipo di pacchetto inoltrato	Risultato	Motivo
Porta L2	Non attendibile	Offerta DHCP unicast/ACK	Eliminato	Lo snooping DHCP impedisce i messaggi del server su porte L2 non attendibili.
Porta L3	N/D (instradato)	Offerta DHCP unicast/ACK	Accettato	Le porte di routing sono i nodi previsti per la comunicazione dell'agente di inoltro.
Porta L2	Attendibile	Rilevamento DHCP unicast con opzione 82	Accettato	Una porta attendibile consente tutti i segnali DHCP.
Porta L2	Non attendibile	Rilevamento DHCP unicast con opzione 82	Accettato	Il pacchetto con indirizzo IP e opzione 82 dell'agente di inoltro è legittimo.
Porta L2	Attendibile	Individuazione DHCP unicast senza opzione 82	Accettato	Una porta attendibile consente tutti i segnali DHCP.
Porta L2	Non attendibile	Individuazione DHCP unicast senza opzione 82	Eliminato	Il pacchetto con indirizzo IP dell'agente di inoltro e nessuna opzione 82 è anomalo.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).