

# Risoluzione dei problemi relativi agli endpoint Catalyst serie 9000 che non ricevono l'indirizzo DHCP quando reindirizzati da ISE

## Sommario

---

---

## Problema

Dopo aver abilitato l'autenticazione con il reindirizzamento da Cisco Identity Services Engine (ISE) su uno switch Cisco Catalyst serie 9000, gli endpoint con cavo non sono in grado di ottenere gli indirizzi IP tramite il protocollo DHCP (Dynamic Host Configuration Protocol) in modo intermittente. Non vengono rilevati problemi sugli switch non Catalyst serie 9000 con le stesse configurazioni.

## Ambiente

- Famiglia di prodotti: Catalyst serie 9000
- Computer Windows con errori di acquisizione DHCP
- L'elenco di controllo di accesso (ACL) reindirizzato sullo switch Catalyst serie 9000 non nega esplicitamente il traffico DHCP

## Risoluzione

1. Aggiungere le seguenti istruzioni deny all'ACL di reindirizzamento per gestire in modo esplicito il traffico DHCP:

```
nega udp any eq bootps any
```

```
nega udp qualsiasi bootpc eq
```

```
negate ip bootpc eq udp any
```

2. Dopo aver modificato l'ACL, autenticare nuovamente un dispositivo che in precedenza aveva generato un errore per verificare che ora possa recuperare un indirizzo IP tramite DHCP.

## Causa

Quando l'autenticazione è abilitata, gli switch Catalyst serie 9000 elaborano i pacchetti in modo diverso dai modelli di switch precedenti. Sugli switch Catalyst serie 9000, l'ordine di elaborazione dei pacchetti è il seguente:

1. I pacchetti che soddisfano una regola ACE (Access Control Entry) di autorizzazione vengono inviati alla CPU per il reindirizzamento al server AAA.
2. I pacchetti che soddisfano una regola di negazione dell'accesso vengono inoltrati tramite il commutatore.
3. I pacchetti che non soddisfano le regole ACE di autorizzazione o di negazione vengono elaborati dal successivo elenco di controllo di accesso scaricabile (DACL, Downloadable Access Control List) e, se non esiste alcun DACL, i pacchetti raggiungono l'ACL di negazione implicita e vengono scartati.

Questo metodo di elaborazione è diverso dai vecchi modelli di switch che usano ACL predefiniti, che permettono il traffico DHCP per impostazione predefinita, e vengono elaborati prima di reindirizzare gli ACL. I modelli Catalyst serie 9000 non usano questi ACL predefiniti e si basano interamente sugli ACL di reindirizzamento e DACL in uso nella sessione. Di seguito è riportato l'ACL predefinito per le sessioni in modalità chiusa sugli switch Catalyst precedenti:

```
3750#sh ip access-lists Auth-Default-ACL
```

```
Auth-Default-ACL elenco accessi IP estesi
```

```
10 consenti udp qualsiasi intervallo bootps 65347 qualsiasi intervallo bootpc 65348 (22 corrispondenze)
```

```
20 consenti udp per qualsiasi intervallo bootps 65347 (12 corrispondenze)
```

```
30 deny ip any any
```

## Contenuto correlato

- [ACL predefiniti per autenticazione 802.1X](#)
- [Supporto tecnico Cisco e download](#)

## 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).