Troubleshoot Catalyst 9000 Series Endpoints Not Receiving DHCP Address when Redirected by ISE

Contents

Issue

After enabling authentication using redirection from Cisco Identity Services Engine (ISE) on a Cisco Catalyst 9000 series switch, wired endpoints are intermittently unable to obtain IP addresses through Dynamic Host Configuration Protocol (DHCP). No issues are observed on non Catalyst 9000 Series switches using the same configurations.

Environment

- Product Family: Catalyst 9000 Series
- Windows computers experiencing DHCP acquisition failures
- Redirect Access Control List (ACL) on the Catalyst 9000 Series switch does not explicitly deny DHCP traffic

Resolution

1. Add the following deny statements to the redirect ACL to explicitly handle DHCP traffic:

```
deny udp any eq bootps any

deny udp any any eq bootpc

deny udp any eq bootpc any
```

2. After modifying the ACL, re-authenticate a previously failing device to verify that it can now successfully retrieve an IP address through DHCP.

Cause

The Catalyst 9000 series switches process packets differently than older switch models when authentication is enabled. The packet processing order on Catalyst 9000 series switches is as follows:

1. Packets that match a permit Access Control Entry (ACE) rule are sent to the CPU for redirection to the AAA server.

2. Packets that match a deny ACE rule are forwarded through the switch.

3. Packets that match neither permit nor deny ACE rules are processed by the next Downloadable Access Control List (DACL), and if no DACL exists, packets hit the implicit-deny ACL and are dropped.

This processing method differs from older switch models that use default ACLs which allow DHCP traffic by default and are processed before redirect ACLs. Catalyst 9000 series models do not use these default ACLs and instead rely entirely on the redirect ACL and DACL in place on the session. The default ACL for closed mode sessions on predecessor Catalyst switches follows:

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

Extended IP access list Auth-Default-ACL

10 permit udp any range bootps 65347 any range bootpc 65348 (22 matches)

20 permit udp any any range bootps 65347 (12 matches)

30 deny ip any any
```

Related Content

- Default ACLs for 802.1X Authentication
- Cisco Technical Support & Downloads