Segment ID Support for DHCP Relay

Feature Information for Segment ID

Table 1: Feature Information for Segment ID

Feature	Releases	Feature Information
DHCP	7.2(0)D1(1)	Included a new chapter on *Segment ID Support for DHCP Relay* . DHCP relay configuration.
DHCP Server	7.2(0)N1(1)	Included a new section on *Configuring Windows 2012 as DHCP Server* . Support common DHCP-Servers for IP address assignments within DFA.

Segment ID Support for DHCP Relay

This feature explains how a Cisco Nexus 7000 Series Switches perform the role of a DHCP relay in the DFA environment.

Note A detailed explanation of the DHCP feature documentation for Cisco Nexus 7000 Series Switches is available in the Configuring DHCP chapter of the *Cisco Nexus 7000 Series NX-OS Security Configuration Guide*.

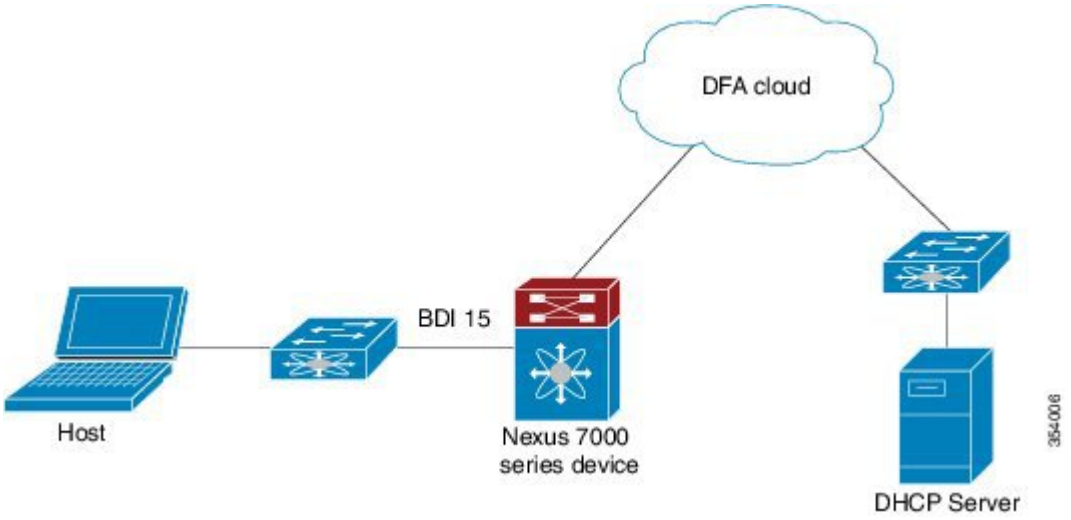
Guidelines and Limitations

- You should know about the DHCPv4 relay, DHCPv6 relay, BDI, and segment ID functions.

Information About Segment ID Support for DHCP Relay

DHCP Relay Configuration Overview

Figure 1: DHCP relay configuration through a BDI



The illustration depicts a Cisco Nexus 7000 Series Switches in a DFA environment (*Nexus 7000)*. The DHCP client (*Host*) seeking an IP address via DHCP is on the left side and the DHCP server that provides the IP address is on the right side (*DHCP Server*). Here, we configure the DHCP server address on a BDI of the Cisco Nexus 7000 Series Switch.

The following sections explain DHCP relay configuration:

1. Enabling a Cisco Nexus 7000 Series Switch as a DHCP relay agent.
2. Configuring a DHCP server address on the relay agent.
3. Configuring the VPN option for the DHCP relay agent.

Enabling a Cisco Nexus 7000 Series Switch as a DHCP Relay Agent

Enabling a Device as a DHCPv4 Relay Agent

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ip dhcp relay
```

Enabling a Device as a DHCPv6 Relay Agent

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ipv6 dhcp relay
```

Configuring a DHCP server address on the Relay Agent

Configuring a DHCPv4 Server Address on the Relay Agent

```
switch(config)# interface bdi 15
switch(config-if)# ip dhcp relay address 192.0.2.120 use-vrf management
```

- The interface level configuration command (**ip dhcp relay address**) is used to configure or disable a server address on a BDI.
- The **use-vrf** option is used to specify the VRF name of the server if the client and server are in different VRFs.

Configuring a DHCPv6 Server Address on the Relay Agent

```
switch(config)# interface bdi 15
switch(config-if)# ipv6 dhcp relay address 2001:DB8:1::1 use-vrf management2
```

- The interface level configuration command (**ipv6 dhcp relay address**) is used to configure or disable a server address on a BDI.
- The **use-vrf** is used to specify the VRF name of the server if the client and server are in different VRFs.
- The server address can either be a link scoped unicast or multicast address, or it can be a global or site local unicast or multicast address.
- An interface is required when the DHCP server address is a link local address or multicast address. It is not allowed for a unicast address.

Important You should be able to ping the server (for the specified server address) from the specified VRF.

Configuring the VPN option for the Relay Agent

Attention In a DFA environment with DHCP Relay, configuring the **vpn** option is mandatory. After configuring the **vpn** option, the DHCP server may be placed within the same or different VRF (default or management).

Configuring the VPN option for the DHCPv4 Relay Agent

```
switch# configure terminal
switch(config)# ip dhcp relay information option
switch(config)# ip dhcp relay information option vpn
```

- The global level **vpn** configuration command is used to enable or disable the DHCPv4 relay function within or across VRFs.

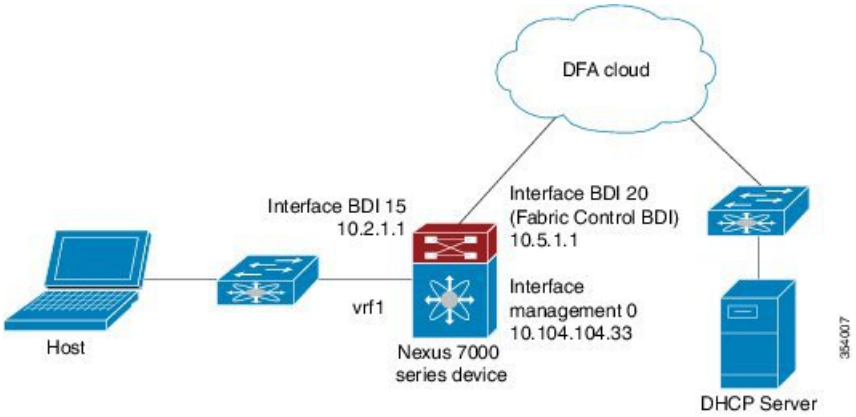
Configuring the VPN option for the DHCPv6 Relay Agent

```
switch# configure terminal
switch(config)# ipv6 dhcp relay option vpn
```

- The global level configuration command is used to enable or disable the DHCPv6 relay function across VRFs. When this is enabled, and the DHCPv6 server is in a different VRF, the relay agent inserts a virtual selection sub option in the *relay-forward* message. By default, this is disabled.

After DHCP relay configuration on a device and assignment of a DHCP server address through a BDI, the network topology looks like this:

Figure 2: DHCP relay configuration and DHCP server address assignment through a BDI



Configuring Windows 2012 as DHCP Server

You can have common DHCP-Servers (for example, Microsoft Windows) for IP address assignments within DFA. The DHCP-Servers can assign IP addresses to a simple DHCP request. The common DHCP-Server support does not rely on specific DHCP scope option (for example, simple-mode) by accepting some limitations or additional configuration.

We support Windows 2012 DHCP server by utilizing the 'Super Scope' as well as the policy on option 82 for address range selection. The DHCP policy on scope reserves the address space exclusively for the request matching the policy.

Note We support both Windows DHCPv4 and DHCPv6 servers and the configurations are similar to regular networks.

Let us assume the switch is using the address from subnet B (it can be the backbone subnet, management subnet, or any customer designated subnet for this purpose) to communicate with the Windows DHCP server. In DFA we have subnets S1, S2, S3, …, Sn for segment s1, s2, s3, …, sn.

To configure DHCP on Windows server.

1. Create a super scope. Within the super scope, create scope B, S1, S2, S3, …, Sn for the subnet B and the subnets for each segment.
2. In scope B, specify the 'Exclusion Range' to be the entire address range (so that the offered address range must not be from this scope).
3. For every segment scope Si, specify a policy that matches on Agent Circuit ID with value of '0108000600XXXXXX', where '0108000600' is a fixed value for all segments, the 6 numbers "XXXXXX" is the segment ID value in hexadecimal. Also ensure to check the **Append wildcard(*)** check box.
4. Set the policy address range to the entire range of the scope.

Configuring Infoblox as DHCP Server

Uses the Link Selection sub-option for scope selection, as this is by default set as the client facing SVI address. For other DHCP servers such as DHCPd and CPNR, GIAddr based scope selection is used. If you are already using Infoblox, then you must upgrade the Cisco NX-OS Switch to version 7.1(1)N1(1) or later.

Note We support only DHCPv4 for Infoblox and the configurations are similar to regular networks. You can refer to Infoblox user manual for configuration.

Let us consider a case where, the DHCP clients are VM hosts connecting to Cisco switches in DFA. The switches are configured with SVI as gateway for the VM hosts. The IP address of the SVI may not be unique in the DFA system, as when VM host moves to server connecting to another switch, then another SVI will be brought up on that switch and configured with the same gateway IP so that the VM does not need to change its gateway IP.

Configuring DHCPd as DHCP Server

The system has a centralized DHCP server that serves all VM hosts. Every switch has a DHCP relay agent running to forward the DHCP requests from VM hosts to the DHCP server. Because the SVI IP address is not unique, hence not reachable from the DHCP server, the relay agent on switch cannot use it as the GIAddr in the request. Instead, it uses another routing interface which has unique IP address as GIAddr. In order for the DHCP server to select the correct subnet for each host, the relay agent also put an identifier in the Circuit ID field in the Relay Agent Information option. The identifier uniquely identifies the subnet that a host connects to. However the identifier is only a portion of the Circuit ID.

Now on the DHCP server, you must configure it to fetch the identifier out of the Circuit ID and use the identifier to choose the right subnet. We are able to do this with DHCPd in the following way: we define classes matching on substring of the Circuit ID. All the host subnets are in a shared-network. The shared-network also contains the subnet for the routing interfaces on the switch, so that the shared-network will be picked when the request comes. The subnet for the routing interfaces does not have address pool, so it will not assign addresses. The address allocation is from the host subnets in the shared-network. Each host subnet only allows its own class members. Hence the server can correctly choose a subnet for address allocation based on the identifier carried in the request.

An example of the DHCPd configuration is given below. Here '59.2.8.0/24' and '99.1.3.0/24' are the host subnets, with identifier '01:5f:91' and '01:5f:92' respectively. Subnet '43.2.0.0/24' is the subnet of the routing interfaces. It is used to select the shared-network, but not used for address allocation.

```
# Start Segment 90001
class "15f91" {
match if substring (option agent.circuit-id, 5, 3) =01:5f:91;
}
# End Segment 90001

# Start Segment 90002
class "15f92" {
match if substring (option agent.circuit-id, 5, 3) =01:5f:92;
}
# End Segment 90002

shared-network "dfa-network" {

# Start Segment primarySubnet
subnet 43.2.0.0 netmask 255.255.255.0 {
```

```
}
# End Segment primarySubnet

# Start Segment 90001
subnet 59.2.8.0 netmask 255.255.255.0 {
option routers 59.2.8.1;
option vlan-id 90001;
 }
 pool {
allow members of "15f91";
range 59.2.8.2 59.2.8.254;
}
# End Segment 90001

# Start Segment 90002
subnet 99.1.3.0 netmask 255.255.255.0 {
option routers 99.1.3.1;
option vlan-id 90002;
 }
 pool {
allow members of "15f92";
range 99.1.3.2 99.1.3.254;
}
# End Segment 90002

}
```