

DHCP Tunnels Support

The DHCP Tunnels Support feature provides the capability to configure the node (or spoke) of the generic routing encapsulation (GRE) tunnel interfaces dynamically using DHCP.

In a Dynamic Multipoint VPN (DMVPN) network, each participating spoke must have a unique IP address belonging to the same IP subnet. It is difficult for a network administrator to configure the spoke addresses manually on a large DMVPN network. Hence, DHCP is used to configure the spoke address dynamically on a DMVPN network.

- Restrictions for DHCP Tunnels Support, on page 1
- Information About DHCP Tunnels Support, on page 2
- How to Configure DHCP Tunnels Support, on page 3
- Configuration Examples for DHCP Tunnels Support, on page 5
- Additional References, on page 6
- Feature Information for DHCP Tunnels Support, on page 7

Restrictions for DHCP Tunnels Support

- The DHCP functionality of address validation is not supported on DMVPN.
- The DHCP IP address is not assigned to the spoke when configured in DMVPN phase 1.
- When you register the spoke to the hub using the `ip nhrp nhs {dynamic nbma nbma-address | FQDN-string} [multicast]` command, the unicast adjacency is only created after the session comes up.
- When using the Dual-hub single-DMVPN topology, Cisco DHCP server automatically changes the unicast flag to broadcast mode. To prevent this automatic change, run the following command on the Cisco DHCP server:

  ```
  no ip dhcp auto-broadcast
  ```

- When DHCP is configured on an interface, the interface may take more time than usual to shutdown.

Information About DHCP Tunnels Support

DHCP Overview

DHCP is based on the Bootstrap Protocol (BOOTP), which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability to automatically allocate reusable network addresses and configuration options to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. See the "DHCP" section of the *Cisco IOS IP Addressing Configuration Guide* for more information.

DHCP Behavior on a Tunnel Network

DMVPN spoke nodes establish a tunnel with a preconfigured DMVPN next hop server (NHS) (hub node) and exchange IP packets with the NHS before an IP address is configured on the tunnel interface. This allows the DHCP client on the spoke and the DHCP relay agent or the DHCP server on the NHS to send and receive the DHCP messages. A DHCP relay agent is any host that forwards DHCP packets between clients and servers.

When the tunnel on a spoke is in the UP state or becomes active, the spoke establishes a tunnel with the preconfigured hub node. The tunnel formation may include setting up IP Security (IPsec) encryption for the tunnel between the spoke and the hub. DHCP receives the GRE tunnel interface UP notification only after the spoke establishes a tunnel with the hub. The DHCP client configured on the spoke must exchange the DHCP IP packets with the hub (DHCP relay agent or server) to obtain an IP address for the GRE tunnel interface. Therefore, the spoke-to-hub tunnel must be in active state before the GRE tunnel interface UP notification is sent to the DHCP server or the relay agent.

IP packets that are broadcast on the DMVPN spoke reach the DMVPN hub. The spoke broadcasts a DHCPDISCOVER message to the DHCP relay agent on the DMVPN hub, before the spoke has an IP address on the GRE tunnel interface. By using the DHCPDISCOVER message, DHCP unicasts the offer back to the client. The hub cannot send IP packets to the spoke before the hub receives a Next Hop Resolution Protocol (NHRP) registration from the spoke. The DHCP relay agent configured on the DMVPN hub adds mapping information to the DHCP client packets (DHCPDISCOVER and DHCPREQUEST).

Depending on whether the hub is a DHCP server or a DHCP relay agent, the mapping is handled differently.

- If the hub is a DHCP server, the Non-Broadcast Multiple Access (NBMA) address is known and a temporary mapping is created on the hub. The hub then unicasts a reply to the spoke.
- If the hub is a DHCP relay agent, the server behind the relay assigns the address. To preserve the NBMA address of the spoke, the address is attached to the DHCP message. When the reply is received, the NBMA address is fetched from the message. The address is sent to the spoke to create the mapping.



Note The NHRP registration sent by the spoke is suppressed until DHCP obtains an address for the GRE tunnel interface. Hence allows reliable exchange of standard DHCP messages.

DMVPN Hub as a DHCP Relay Agent

Relay agents are not required for DHCP to work. Relay agents are used only when the DHCP client and server are in different subnets. The relay agent acts as a communication channel between the DHCP client and server. The DHCP--Tunnels Support feature requires the DMVPN hub to act as a relay agent to relay the DHCP messages to the DHCP server.

The DHCP server is located outside the DMVPN network and is accessible from the DMVPN hub nodes through a physical path. The spoke nodes reach the DHCP servers through the hub-to-spoke tunnel (GRE tunnel). The DHCP server is not directly reachable from the DMVPN spoke. The DHCP relay agent on the DMVPN hub helps the DHCP protocol message exchange between the DHCP client on the spoke and the DHCP server.

DMVPN Topologies

Dual-Hub Single-DMVPN Topology

In a dual-hub single-DMVPN topology, both the hubs must be connected to the same DHCP server that has the high availability (HA) support to maintain DMVPN redundancy. If the hubs are connected to different DHCP servers, they must be configured with mutually exclusive IP address pools for address allocation.

Dual-Hub Dual-DMVPN Topology

In the dual-hub dual-DMVPN topology, each hub is connected to a separate DHCP server. The DMVPN hubs (DHCP relay agents) include a client-facing tunnel IP address in the relayed DHCP requests. DHCP requests are used by the DHCP server to allocate an IP address from the correct pool.

Hierarchical DMVPN Topology

In a DMVPN hierarchical topology, there are multiple levels of DMVPN hubs. However, all the tunnel interface IP addresses are allocated from the same IP subnet address. The DHCP client broadcast packets are broadcast to the directly connected hubs. Hence, the DMVPN hubs at all levels must either be DHCP servers or DHCP relay agents. If DHCP servers are used then the servers must synchronize their databases. The DMVPN hubs must be configured as DHCP relay agents to forward the DHCP client packets to the central DHCP servers. If the DHCP server is located at the central hub, all DHCP broadcasts are relayed through the relay agents until they reach the DHCP server.

How to Configure DHCP Tunnels Support

Configuring the DHCP Relay Agent to Unicast DHCP Replies

Perform this task to configure the DHCP relay agent (hub) to unicast DHCP replies.

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. Therefore a bandwidth burst occurs. The DHCP Tunnels Support feature does not function if the DHCP messages are broadcast. Hence, you must configure the DHCP relay agent to unicast the DHCP messages for the DHCP to be functional in a DMVPN environment.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp support tunnel unicast**
4. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp support tunnel unicast** **Example:** `Router(config)# ip dhcp support tunnel unicast`	Configures a spoke-to-hub tunnel to unicast DHCP replies over the DMVPN network.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring a DMVPN Spoke to Clear the Broadcast Flag

Perform this task to configure a DMVPN spoke to clear the broadcast flag.

By default, DMVPN spokes set the broadcast flag in the DHCP DISCOVER and REQUEST messages. Therefore the DHCP relay agent is forced to broadcast the DHCP replies back to the spokes, even though the relay agent has sufficient information to unicast DHCP replies. Hence, you must clear the broadcast flag from the DMVPN spoke.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip dhcp client broadcast-flag clear**
5. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 1`	Configures a tunnel interface and enters interface configuration mode.
Step 4	**ip dhcp client broadcast-flag clear** **Example:** `Router(config-if)# ip dhcp client broadcast-flag clear`	Configures the DHCP client to clear the broadcast flag.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Configuration Examples for DHCP Tunnels Support

Example: Configuring a DHCP Relay Agent to Unicast DHCP Replies

The following example shows how to configure a DHCP relay agent to unicast DHCP replies:

```
Device# configure terminal
Device(config)# ip dhcp support tunnel unicast
Device(config)# exit
.
.
.
```

Example: Configuring a DMVPN Spoke to Clear the Broadcast Flag and Set the IP Address to DHCP

The following example shows how to configure a DMVPN spoke to clear the broadcast flag and set the IP address to DHCP:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip dhcp client broadcast-flag clear
Device(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS security commands	*Cisco IOS Security Command Reference*
Cisco IOS IP addressing configuration tasks	*Cisco IOS IP Addressing Configuration Guide*
Cisco IOS IP addressing services commands	*Cisco IOS IP Addressing Services Command Reference*

Standards

Standard	Title
--	No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2131	*Dynamic Host Configuration Protocol*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCP Tunnels Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for DHCP-Tunnels Support

Feature Name	Releases	Feature Information
DHCP--Tunnels Support	Cisco IOS XE Release 16.12	The DHCP--Tunnels Support feature provides the capability to configure the node (or spoke) of the GRE tunnel interfaces dynamically using DHCP. The following commands were introduced or modified: **ip address dhcp**, **ip dhcp client broadcast-flag**, **ip dhcp support tunnel unicast**.