DHCP Server MIB

The DHCP Server MIB feature provides Simple Network Management Protocol (SNMP) access to and control of Cisco IOS Dynamic Host Configuration Protocol (DHCP) server software on a Cisco router by an external network management device.

- Prerequisites for the DHCP Server MIB, on page 1
- Information About the DHCP Server MIB, on page 1
- How to Enable DHCP Trap Notifications, on page 6
- Configuration Examples for the DHCP Server MIB, on page 8
- Additional References, on page 9
- Feature Information for DHCP Server MIB, on page 11

Prerequisites for the DHCP Server MIB

SNMP must be enabled on the router before DHCP server trap notifications can be configured.

Information About the DHCP Server MIB

SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

SNMP defines two main types of entities: managers and agents. The SNMP manager is a system that controls and monitors the activities of network hosts using SNMP. The agent is the software component within a remote networking device that maintains the data and reports this data, as needed, to the manager. The manager and agent share a Management Information Base (MIB) that defines the information that the agent can make available to the manager.

An important feature of SNMP is the capability to generate unsolicited notifications from an SNMP agent. These trap notifications are messages alerting the SNMP manager to conditions on the network. Traps are considered an agent-to-manager function and a request for confirmation of receipt from the SNMP manager is not required.

DHCP Server Trap Notifications

DHCP server trap notifications are sent to the SNMP manager for the following events:

- Address utilization for a subnet has risen above or fallen below a configurable threshold.
- Address utilization for an address pool has risen above or fallen below a configurable threshold.
- A lease limit violation is detected. The lease limit configuration allows you to control the number of subscribers per interface.
- The DHCP server has started or stopped.
- A duplicate IP address is detected.

The DHCP Server MIB feature does not send the same type of trap notification back-to-back for the same threshold event. For example, if the low threshold value for available free addresses becomes equal to or less than the configured value, a free address low event trap notification on the subnet or pool is generated. This same trap notification will not be resent until the value for the available free addresses has exceeded the value of the free high threshold and vise versa. This threshold control mechanism applies to all trap notifications concerning thresholds in addition to the trap notifications for the DHCP server start and stop time and the lease limit violation. The duplicate IP address trap notification is not subject to this threshold control mechanism.

Tables and Objects in the DHCP Server MIB

The DHCP Server MIB consists of the following tables and objects. The first character of a row in the table begins with "c" (Cisco) and is mapped to the object defined in the IETF draft RFC, *Dynamic Host Configuration Protocol for IPv4 Server MIB.* If the information is not currently available in Cisco IOS software, the value in the second column is displayed as 0 (zero).

- cDhcpv4SrvSystemsObjects (see Table 7)--System description and object IDs
- cBootpHCCounterObjects (see Table 8)--BOOTP counter information
- cDhcpv4HCCounterObjects (see Table 9)--DHCPv4 counter information
- cDhcpv4ServerSharedNetTable (see Table 10)--DHCP address pool information
- cDhcpv4ServerSubnetTable (see Table 11)--Additional DHCP address pool subnet information including secondary subnet information
- cDhcpv4SrvExtSubnetTable (see Table 12)--Additional DHCP address pool subnet information
- cDhcpv4ServerNotifyObjectsGroup (see Table 13)--This objects group is used by the cDhcpv4ServerNotificationsGroup notifications group.
- cDhcpv4ServerNotificationsGroup (see Table 14)--This notifications group consists of all traps defined in the Cisco IOS DHCP server.
- cDhcpv4SrvExtNotifyGroup (see Table 15)--This notifications group consists of all traps not defined in the draft DHCPv4 Server MIB RFC.

Table 1: cDhcpv4SrvSystemsObjects and Descriptions

Name	Description
cDhcpv4SrvSystemDescr	Contains a textual description of the server (full name and version identification).
cDhcpv4SrvSystemObjectID	Cisco experiment node for the DHCP Server MIB. For example, 1.3.6.1.4.1.9.10.102...

Table 2: cBootpHCCounterObjects and Descriptions

Name	Description
cBootpHCCountRequests	The number of packets received that do contain a BOOTREQUEST message type in the first octet.
cBootpHCCountInvalids	0
cBootpHCCountReplies	The number of packets received that contain a BOOTREPLY message type in the first octet.
cBootpHCCountDroppedUnknown Clients	0
cBootpHCCountDroppedNotServingSubnet	0

Table 3: cDhcpv4HCCounterObjects and Descriptions

Name	Description
cDhcpv4HCCountDiscovers	The number of DHCPDISCOVER packets received.
cDhcpv4HCCountOffers	The number of DHCPOFFER packets sent.
cDhcpv4HCCountRequests	The number of DHCPREQUEST packets sent.
cDhcpv4HCCountDeclines	The number of DHCPDECLINE packets sent.
cDhcpv4HCCountAcks	The number of DHCPACK packets sent.
cDhcpv4HCCountNaks	The number of DHCPNACK packets sent.
cDhcpv4HCCountReleases	The number of DHCPRELEASE packets sent.
cDhcpv4HCCountInforms	The number of DHCPINFORM packets sent.
cDhcpv4HCCountForcedRenews	0
cDhcpv4HCCountInvalids	The number of DHCP packets received whose DHCP message type is not understood or handled by the DHCP server.
cDhcpv4HCCountDropUnknownClient	0
cDhcpv4HCCountDropNotServingSubnet	0

Table 4: cDhcpv4ServerSharedNetTable and Descriptions

Name	Description
cDhcpv4ServerSharedNetName	The DHCP address pool name.
cDhcpv4ServerSharedNetFreeAddr LowThreshold	This entry value corresponds to the **utilization mark high** command in DHCP pool configuration mode multiplied by the total pool addresses then divided by 100.
cDhcpv4ServerSharedNetFreeAddrHighThreshold	This entry value corresponds to the **utilization mark low** command in DHCP pool configuration mode multiplied by the total subnet addresses then divided by 100.
cDhcpv4ServerSharedNetFree Addresses	The number of IPv4 addresses that are available within this shared network.
cDhcpv4ServerSharedNetReserved Addresses	The number of IP addresses that are reserved for the pool (not available for assignment). This entry corresponds to the **ip dhcp excluded-address** global configuration command. The value is zero if no excluded addresses are defined for the pool.
cDhcpv4ServerSharedNetTotal Addresses	The number of IP addresses that are available within this shared network.

Table 5: cDhcpv4ServerSubnetTable and Descriptions

Name	Description
cDhcpv4ServerSubnetAddress	The IP address of the subnet entry in the table.
cDhcpv4ServerSubnetMask	The subnet mask of the subnet.
cDhcpv4ServerSubnetSharedNetworkName	The DHCP address pool name to which the subnet belongs.
cDhcpv4ServerSubnetFreeAddrLowThreshold	This entry value corresponds to the **override utilization high** command in DHCP pool secondary subnet configuration mode multiplied by the total subnet addresses then divided by 100.
cDhcpv4ServerSubnetFreeAddrHighThreshold	This entry value corresponds to the **override utilization low** command in DHCP pool secondary subnet configuration mode multiplied by the total subnet addresses then divided by 100.
cDhcpv4ServerSubnetFree Addresses	The number of free IP addresses that are available in the subnet.

Table 6: cDhcpv4SrvExtSubnetTable and Descriptions

Name	Description
cDhcpv4ServerDefaultRouterAddress	The entry corresponds to the **override default-router** command in DHCP pool secondary subnet configuration mode.
cDhcpv4ServerSubnetStartAddress	The first subnet IP address.
cDhcpv4ServerSubnetEndAddress	The last subnet IP address.

Table 7: cDhcpv4ServerNotifyObjectsGroups and Descriptions

Name	Description
cDhcpv4ServerNotifyDuplicateIpAddr	The IP address is found to be a duplicate. Duplicates are detected by servers who send a PING before offering an IP address lease or by a client sending a gratuitous ARP message reported through a DHCPDECLINE message.
cDhcpv4ServerNotifyDuplicateMac	The offending MAC address that caused a duplicate IPv4 address to be detected, if captured by the server, otherwise set to 00-00-00-00-00-00.
cDhcpv4ServerNotifyClientOrServerDetected	This object is set by the server to client if the client used DHCPDECLINE to mark the offered address as in use, or to server if the server discovered that address was in use by a client before offering it.
cDhcpv4ServerNotifyServerStart	The date and time when the server began operation, which is controlled by the **service dhcp** command.
cDhcpv4ServerNotifyServerStop	The date and time when the server ceased operation, which is controlled by **no service dhcp** command.

Table 8: cDhcpv4ServerNotificationsGroup and Descriptions

Name	Description
cDhcpv4ServerFreeAddressLow	This notification signifies that the number of available IP addresses for a DHCP address pool has fallen below the defined low threshold. This notification corresponds to the **snmp-server enable traps dhcp** global configuration command.
cDhcpv4ServerFreeAddressHigh	This notification signifies that the number of available IP addresses for a DHCP address pool has risen above the defined high threshold. This notification corresponds to the **snmp-server enable traps dhcp** global configuration command.
cDhcpv4ServerStartTime	This notification signifies that the server has started. This notification corresponds to the **service dhcp** and **snmp-server enable traps dhcp time**global configuration commands.

Name	Description
cDhcpv4ServerStopTime	This notification signifies that the server has stopped normally. This notification corresponds to the **no service dhcp** and **snmp-server enable traps dhcp time**global configuration commands.
cDhcpv4ServerDuplicateAddress	This notification signifies that a duplicate IP address has been detected. This notification corresponds to the **snmp-server enable traps dhcp duplicate**global configuration command.

Table 9: cDhcpv4SrvNotifyGroup and Descriptions

Name (not in the RFC draft)	Description
cDhcpv4ServerIfLeaseLimitExceeded	This notification signifies that a per interface lease limit is exceeded. This notification corresponds to the **snmp-server enable traps dhcp interface**global configuration command.
cDhcpv4ServerSubnetFreeAddressLow	This notification signifies that the number of available IP addresses for a subnet has fallen below the defined low threshold. This notification corresponds to the **snmp-server enable traps dhcp subnet**global configuration command.
cDhcpv4ServerSubnetFreeAddressHigh	This notification signifies that the number of available IPv4 addresses for a subnet has risen above the defined high threshold. This notification corresponds to the **snmp-server enable traps dhcp subnet**global configuration command.

How to Enable DHCP Trap Notifications

Configuring the Router to Send SNMP Trap Notifications About DHCP

DHCP trap notifications are disabled by default. The trap notification is disabled if the corresponding trap configuration is not enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps dhcp duplicate**] [**interface**] [**pool**] [**subnet**] [**time**
4. **end**

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	**snmp-server enable traps dhcp duplicate**] [**interface**] [**pool**] [**subnet**] [**time** **Example:** `Router(config)# snmp-server enable traps dhcp`	Enables the sending of DHCP SNMP trap notifications. • **duplicate** --Sends notification about duplicate IP addresses. • **interface** --Sends notification that a per interface lease limit is exceeded. • **pool** --Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold. • **subnet** --Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold. • **time** --Sends notification that the DHCP server has started or stopped. • If you specify the **snmp-server enables traps dhcp** command without any of the optional keywords, all DHCP trap notifications are enabled.
Step 4	**end** **Example:** `Router(config)# end`	Returns the router to privileged EXEC mode.

Troubleshooting Tips

If you are using secondary IP addresses under a single loopback interface and using secondary subnets under a DHCP pool, use one DHCP pool to configure networks for all the secondary subnets instead of using one pool per secondary subnet. The **network** *network-number* [*mask* | */prefix-length*] [**secondary**] command must be configured under a single DHCP address pool rather than multiple DHCP address pools.

The following is the correct configuration:

```
!
ip dhcp pool dhcp_1
 network 172.16.1.0 255.255.255.0
 network 172.16.2.0 255.255.255.0 secondary
 network 172.16.3.0 255.255.255.0 secondary
 network 172.16.4.0 255.255.255.0 secondary
!
interface Loopback111
 ip address 172.16.1.1 255.255.255.255 secondary
 ip address 172.16.2.1 255.255.255.255 secondary
 ip address 172.16.3.1 255.255.255.255 secondary
 ip address 172.16.4.1 255.255.255.255 secondary
```

The following is the incorrect configuration:

```
!
ip dhcp pool dhcp_1
 network 172.16.1.0 255.255.255.0
 lease 1 20 30
 accounting default
!
ip dhcp pool dhcp_2
 network 172.16.2.0 255.255.255.0
 lease 1 20 30
 accounting default
!
ip dhcp pool dhcp_3
 network 172.16.3.0 255.255.255.0
 lease 1 20 30
 accounting default
!
ip dhcp pool dhcp_4
 network 172.16.4.0 255.255.255.0
 lease 1 20 30
 accounting default
!
interface Loopback111
 ip address 172.16.1.1 255.255.255.255 secondary
 ip address 172.16.2.1 255.255.255.255 secondary
 ip address 172.16.3.1 255.255.255.255 secondary
 ip address 172.16.4.1 255.255.255.255 secondary
```

Configuration Examples for the DHCP Server MIB

DHCP Server MIB--Secondary Subnet Trap Example

The following example configures 192.0.2.0/24 as the subnetwork number and mask of the DHCP pool named pool2 and then adds the DHCP pool secondary subnet specified by the subnet number and mask 192.0.4.0/30. The IP addresses in pool2 consist of two disjoint subnets: the addresses from 192.0.2.1 to 192.0.2.254 and the addresses from 192.0.4.1 to 192.0.4.2.

The address pool utilization mark, configured at the global level, will be overridden at the secondary subnet level. A trap is sent to the SNMP manager if the subnet size of the secondary subnet exceeds or goes below the level specified by the **override utilization** commands.

The **utilization mark** {**high**| **low**} **log** command enables a system message to be generated for a DHCP address pool or secondary subnet when the utilization exceeds the configured high utilization threshold or falls below the configured low utilization threshold.

```
!
ip dhcp pool pool2
 utilization mark high 80 log
 utilization mark low 70 log
 network 192.0.2.0 255.255.255.0
 network 192.0.4.0 255.255.255.252 secondary
 override utilization high 40
 override utilization low 30
!
snmp-server enable traps dhcp subnet
```

DHCP Server MIB--Address Pool Trap Example

In the following example, if the address utilization exceeds the high threshold or drops below the low threshold, an SNMP trap will be sent to the SNMP manager and a system message will be generated.

```
ip dhcp pool pool3
 utilization mark high 80 log
 utilization mark low 70 log
!
snmp-server enable traps dhcp pool
```

DHCP Server MIB--Lease Limit Violation Trap Example

In the following example, four DHCP clients are allowed to receive IP addresses. If a fifth client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server and a trap will be sent to the SNMP manager.

```
ip dhcp limit lease log
interface Serial 0/0
 ip dhcp limit lease 4
 exit
snmp-server enable traps dhcp interface
```

Additional References

The following sections provide references related to the DHCP Server MIB feature.

Related Documents

Related Topic	Document Title
SNMP configuration tasks	"Configuring SNMP Support" module
DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*

Related Topic	Document Title
DHCP server configuration tasks including subnet utilization tasks	"Configuring the Cisco IOS DHCP Server" module
DHCP per interface lease limit functionality	"Configuring DHCP Services for Accounting and Security" module
DHCP ODAP tasks including address pool utilization tasks	"Configuring the DHCP Server On-Demand Address Pool Manager" module

Standards

Standard	Title
No new or modified standards are supported by this feature.	--

MIBs

MIB	MIBs Link
• CISCO-IETF-DHCP-SERVER-MIB • CISCO-IETF-DHCP-SERVER-EXT-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
Draft RFC: draft-ietf-dhc-server-mib-10.txt	Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Server MIB

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 Server MIB

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 10: Feature Information for DHCP Server MIB

Feature Name	Releases	Feature Information
DHCP Server MIB		The DHCP Server MIB feature provides SNMP access to and control of Cisco IOS DHCP server software on a Cisco router by an external network management device. The following commands were introduced by this feature: **snmp-server enable traps dhcp**and **debug ip dhcp server snmp**.